ЮГОЗАПАДЕН УНИВЕРСИТЕТ “НЕОФИТ РИЛСКИ”

ТЕХНИЧЕСКИ ФАКУЛТЕТ

КАТЕДРА ”КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА И ТЕХНОЛОГИИ”

Автореферат

на

ДИСЕРТАЦИОНЕН ТРУД

За присъждане на образователна и научна степен

ДОКТОР

Докторска програма

Компютърни системи, комплекси и мрежи

Област на висше образование 5. Технически науки, професионално направление 5.3. Комуникационна и компютърна техника и технологии

АНАЛИЗ И СИМУЛАЦИОННО ИЗСЛЕДВАНЕ НА ОСОБЕНОСТИТЕ НА ЛОКАЛНИ МРЕЖИ

Научни ръководители: доц. д-р Алексей Стефанов
доц. д. н. Иван Тренчев

Докторант: Илиян Иванов

Благоевград, 2021 г.

Искам да изкажа своята огромна благодарност на ***доц. д-р инж. Алексей Стефанов***, който ми подаде ръка в изключително труден за него момент. Силата на волята, ерудицията, интелектът и стремежът към доброто, които той притежаваше, енергията, която влагаше в науката и ангажирането на потенциала на младите хора, ми подействаха вдъхновяващо. За мен ще бъде винаги онзи светъл пример, който да следвам по пътя си. Мой дълг за в бъдеще ще е да предам именно това познание – да учиш, да можеш и да се развиваш по един споделен начин – не само за себе си, а да даваш на младите от своята енергия точно толкова, че да запалиш в тях пламъка на истинското влечение към науката, който остава за цял живот.

Бих искал да изразя своята признателност и към ***доц. д. н. Иван Тренчев***, който през цялото време ме насочваше, даваше идеи, кураж и откри пред мен нови хоризонти.

Дисертантът работи в Югозападен университет “Неофит Рилски”. Дисертационният труд е обсъден и насочен за защита на разширено заседание на катедрения съвет на катедра “Комуникационна и компютърна техника и технологии” на „Югозападен университет “Неофит Рилски” на април 2022 г.

Дисертационният труд е с обем от 193 страници. Основният текст е систематизиран в три глави. Извън него са обособени: *Увод, Заключение, Приноси на дисертационното изследване, Справочен апарат, съдържащ: използвана литература.*

Списъците с използваната литература включват 337 източници.

Публичната защита на дисертационния труд ще се състои на 11.04.2022 г. От ..... часа в зала ..... на ЮГОЗАПАДЕН УНИВЕРСИТЕТ “НЕОФИТ РИЛСКИ”, ул. „Иван Михайлов“ №66 Благоевград, 2700

Съдържание

Увод

Безжичните компютърни мрежи са резултат от естествената еволюция на развитие на компютърните системи по отношение на гъвкавостта в използването на изчислителните ресурси и свободата на разположение на потребителите в пространството и времето. Настоящите технологични решения, използвани за безжично предаване на данни, в зависимост от географското разположение на потребителя и разстоянието, на което се предават данните.

Безжичните локални мрежи (Wireless) LAN- WLAN са един от дяловете на безжичните компютърни мрежи, намиращи приложение за реализацията на компютърни комуникации и мрежови приложения в локална област от типа „in-root, in-building or campusarea". Тяхното предназначение е подобно на кабелно базираните LAN - да пренасят кадри с данни между мобилни или фиксирани станции, принадлежащи на мрежата, като се предоставят и следните допълнителни функции :

- Разширяване на традиционните локални мрежи за мобилни устройства.
- Мобилен достъп до корпоративни мрежи.
- Локални мрежи с равностоен достъп от типа Ad Hoc.
- Мостове за отдалечен достъп от типа Inter-LAN Bridge.
- Интегриране на компютри и комуникационни устройства.

При разглеждане на проблемите и параметрите водещи критерии са осигуряването на максимална скорост на предаване на данните и определяне на вероятността за появата на грешки (BER - bit error rate). Практическото предаване на данните обаче се извършва от протоколите, реализиращи достъпа до съобщителната среда (MAC - media access control)

Целта на настоящата разработка е да се направи обзор на най-разпространените методи за достъп до съобщителната среда при WLAN и съответстващите им MAC протоколи, начина на функциониране и изграждане на безжичните мрежи и видоветекомпютърни мрежи.В последните години о развитието на технологиите се увеличии нуждата от различни видове комуникации [1-6]. Един от най-динамичноразвиващите се методи на комуникация е безжичният. Най-голямотопредимство на безжичните комуникации е мобилността наустройствата, която те използват. В последните години се появихамножество безжични стандарти като най-популярните , от които са -Bluetooth , IEEE 802.15.4/ ZigBee, WiFi (802.11*), Wi-Fi Direct. Тези стандарти сапредназначени за безжична връзка, нуждаеща се от средно висока ивисока скорост на предаване на данни [5-12]. За осъществяването на настощата работа са представенипротоколите на достъп при безжичните локални мрежи (WirelessLAN-Wlan) и основните безжични стандарти, а също така и най -разпространените типове микроконтролери. Също така е разгледан и 802.15.4/ZigBee стандарта, като е направено сравнениес останалите безжични стандарти.

Глава първа

Видове и характеристика на компютърните мрежи

Общи сведения

Мрежата представлява два или повече компютъра, свързани един с друг с помощта на необходимия за целта хардуер и програмни средства, позволяващи им да обменят информация помежду си и между други устройства. Хардуерната връзка между отделните компютри и другата, участваща в мрежата периферия може да бъде изградена с помощта на кабели (коаксиални, усукана двойка, оптични), или с помощта на някоя безжична технология (IRDA, Bluetooth). За осигуряването на мрежовата връзка се "грижат множество мрежови протоколи (TCP/IP, NetBEUI, AppleTalk, PPTP, DHCP)[12]. Най-общо казано, има два типа мрежа-LAN (Local Area Network-локална мрежа) и WAN (Wide Area Network-мрежа върху широка област). LAN е мрежа между множество компютри и периферия, физически разположени в една достатъчно малка като размер област-например, в рамките на една или няколко съседни сгради [28].

WAN е мрежа, която може да се простира на огромно разстояние, като главната й цел е да свързва съществуващите LAN в една мрежа. На свой ред, една WAN може да бъде свързана към друга WAN, образувайки по-висше ниво в мрежовата йерархия.

Най-удачният пример за WAN е Интернет. Скоростта на предаването на данни между две мрежови устройства е дин отнай-важните показатели, характеризиращи мрежата и се измерва в брой битове, предадени за една секунда [18-29]. В синхрон с нарастващите скорости на предаване на данни сепоявиха съкращения от типа на Kbps, Mbps, Gbps, означаващи хилядни,

милионни и милиардни битове за секунда.По отношения конструкцията на LAN можете да срещнете множество термини, като основните от тях са:

- тип мрежа - мрежа с равноправен достъп и тип клиент - сървър
- топология - шина, кръгова и звезда
- архитектура - Ethernet, TokenRing

Типове мрежи

В съвременния свят на компютърните технологии е необходима връзката между компютъра и външни устройства, а също така с други компютри и компютърни мрежи. Съществуват няколко вида връзки. Те могат да бъдат жични и безжични. Всеки персонален компютър е обикновено снабден с два серийни и един паралелен порт. Серийните и паралелните интерфейси работят поразличен начин.Връзката между електронните устройства може да се осъществи по два начина. Възможно е използването на кабели като преносваща среда или безжични технологии.

Жичните интерфейси се използват предимно при настолните компютри. Но с навлизането все повече на портативните компютри и умните мобилни телефони се налага развитието на безжичните стандарти за предаване на данни [18, 28-42].

Класификация според начина на предаване :

Серийни

Серийните портове изпращат един бит по преносната среда. Въпреки, че е нужно пращането на бит по бит по преносната среда, броят на проводниците е значително по - малък .

Има два основни вида серийни комуникации - синхронни и асинхронни [28, 35, 78].

Синхронните интерфейси обменят информация относно синхронизацията преди започването на трансфера, но също така и по време

на него обменят синхронизиращи сигнали [28, 31-38]. Синхронните трансфери позволяват по-висока скорост на обмен от асинхронните.

Асинхронна комуникация означава такава, при която няма синхронизация [45- 62]. Не се изпращат “празни” битове. Серийният порт на персоналните компютри е асинхронен. Въпреки че няма синхронизация, началото и края на всеки предаден байт трябва да бъде обозначен. Това се извършва посредством стартови и стопиращи битове.

Паралелни

Паралелните портове изпращат и приемат информация като предават 8 бита данни едновременно по кабел състоящ се от 8 проводника. Този начин позволява много бърза комуникация, но използвания кабел е неудобен, защото е по - дебел и съставен от много проводници. Паралелните портове се използват най-вече за връзка на компютъра с принтер.

Класификация според правата на свързаните компютри

Съществуват два основни типа локални мрежи, различаващи се по това, какви права имат свързаните в мрежата компютри и по кой начин ги получават. В мрежа с равноправен достъп всеки компютър има равни с другите права, докато в една мрежа тип клиент-сървър тъкмо сървъра определя правата за достъп до другите участници в мрежата при подадена заявка от всеки един компютър-клиент. Между другото, една локална мрежа може да бъде комбинация от двата типа [25, 78-91].

Мрежа с равноправен достъп.

Както следва от наименованието на този тип мрежи,всички участници в нея са равнопоставени, и в един моментедин компютър може да действа като сървър, а в друг-като клиент. Достъпътдообщите мрежови ресурси не сеадминистрира от отделен сървър, както е при мрежите тип клиент-сървър. Този тип мрежи се използва, когато броят компютри е сравнително малък и няма нужда от

централизирано съхраняване на файлове и мрежови приложения. Поддръжката на този тип мрежа е вградена във всички версии на операционните системи на Microsoft: 95,98,Me, 2000, XP,Vista, 7, 8, 8.1, 10 включително и в Home edition [5, 8, 15, 69, 128, 159]. Към другите предимства на този тип мрежи можем да отнесем ниската цена на изграждане, лесното администриране на всеки отделен компютър (възел), липсващата необходимост от мрежов системен администратор, който би трябвало да се грижи за конфигурирането и администрирането.

Мрежа тип клиент-сървър

В този тип мрежи предназначението на отделните машини е фиксирано от самото начало може да има един (или няколко) сървър(а), управляващ(и) достъпа до ресурси и услуги на свързаните към него работни станции.На сървъра могат централизирано да се съхраняват файлове и приложения, достъпни за използване от всеки компютър, което предполага, че ако сървъра е включен, всеки от компютрите-клиенти може да получи достъп до файловете във всеки един момент. В мрежите с равноправен достъп [126-158], при положение, че файловете са споделени (sharing) на някой от компютрите, има изискване той да не се спира, за да осигурява достъпа до определената информация.Нивото на сигурност в една машина от този тип може да бъде относително лесно повишено благодарение на централизиранотоуправление, обикновено извършвано от мрежовия администратор, който, освен това, може да се грижи и за централизирано архивиране на данните, инсталирането на приложения, администрирането на потребителите и т.н [12, 158, 225, 321]. Мрежите от този тип освен, че са по-бързи от мрежите с равноправен достъп, позволяват включването на повечеустройства (не само компютри, но и мрежови принтери и др.), достъпът докоито е по-бърз, отколкото при мрежите с равноправен достъп. От друга страна, оборудването заизграждане на този тип мрежи

е в пъти по - скъпо, за изграждането и администрирането им е необходим мрежов администратор, който, освен всичко друго, трябва да се занимава и с въпросите на сигурността, особено ако мрежата е свързана към Интернет или към друга мрежа.

Комбиниран тип мрежи

Както сигурно се досещате, този тип мрежи е комбинация от горните два типа-мрежа с равноправен достъп и мрежа клиент- сървър. Много често поради спецификата на задачите, които се изпълняват в рамките на една организация, този тип мрежи е за предпочитане [12, 56, 89, 90 -94]

Фигура 1 Комбиниран тип мрежа

Както се вижда от схемата, една обособена част от мрежовите устройства, образуващи работна група, образуват мрежа с равноправен достъп, в която ресурсите се споделят между тях, без да се ангажира сървъра [12, 54, 58, 95-112]. Същевременно, същите компютри са свързани и към сървър, който е част от мрежа тип клиент-сървър. Така, от една страна

сървърът контролира първостепенните ресурси, необходими на цялата мрежа, а от друга, не отделя ресурси за управлението на устройства, необходими за работата само на компютрите от работната група, свързани в мрежа с равнопоставен достъп[1].

Модел OSI

Този модел, OSI (Open System Interconnect), разработен от международната организация за стандартизация ISO описва структурата на една идеална мрежова връзка [45, 58, 69, 226], използвайки понятието нива на взаимодействие на мрежовите компоненти. Моделът OSI съдържа седем нива на взаимодействие, които са относително автономни и могат да се разграничават[2].

Фигура 2 Нива на мрежовите въздействие на компоненти

НИВО	ОЗНАЧЕНИЕ	
1	Физическо	
2	Канално	Media access control
		local link control
3 1	Мрежово	
4	Транспортно	
5	Сесийно	
6	Представително	
7	Приложно	

1. Физическо ниво - отговаря за приемането и предаването на бинарните данни. Това ниво определя електрическите, механическите и процедурните характеристики на канала

[1] https://www.it.souprovadia.info/node/29
[2] http://pencho.my.contact.bg/start/comp/lan/lan.htm

между крайните системи. Точно спецификациите [128, 128, 229] на физическото ниво определят нивата на напреженията, скоростта на предаване на физическата информация, фиксира изискванията за средата за предаване на информация и т.н.

2. Канално ниво - осигурява транспортирането на данните под физическото ниво, подсигурявайки физическата адресациямрежовата топология, информиране за неизправности, администрирането на информационният поток.

3. Мрежово ниво-отговаря за избор на маршрута между двете крайни устройства, дори те да се намират в различни географски райони, за разлика от физическото ниво, което следи само близкостоящите мрежови връзки.

4. Транспортно ниво - най-високо в йерархията на нивата, отговарящи за транспорта на данни. Осигурява следенето за цялостност на изпращаните или получаваните данни, контролира потока и последователността на пакетите с данни, осигурява механизмите за функционирането на виртуалните канали и системите за откриване и отстраняване на неизправности [228, 229, 289, 291].

5. Сесийно ниво - на основата на множество мрежови протоколи установява, управлява и затваря сеансите за взаимодействие между приложенията, администрирайки заявките им.

6. Представително ниво - осигурява "читаемост" на информацията, изпращана от представителното ниво на една система към същото ниво на друга система. За целта това ниво може да транслира изпращаната информация към някакъв общ формат, разбираем за другата система [128 -139].

7. Приложно ниво - осигурява изпълнението на потребителските задачи, служейки за интерфейс между крайният системен потребител и

мрежовите услуги. На това ниво се синхронизират съвместно работещите приложения, идентифицират се устройствата, с които ще се установява връзка, оценява обемът на ресурсите, необходими за предполагаемата връзка [128, 145, 156].

Wireless LAN (безжични комуникационни устройства)

Безжични мрежи

Доскоро, споменавайки този термин, веднага се досещахме за мобилните телефони. Но има и други области, където удобството на безжичните комуникации ги е изтласкало на гърба на комуникационната вълна.

Използването на радиоканалите за връзка между устройствата макар, че не е ново като изобретение, едва напоследък еволюира значително, особено благодарение на широкото разпространение на Internet, локалните и WAN мрежи, свързващи много хора[3], позволяващи да си разменят глас, видео и данни помежду си, и то с осезаемо високи скорости [140- 167].

Тласък за развитието именно на безжичните устройства е дала необходимостта от по-голяма свобода и удобство при изграждането на мрежи, необходимостта от лесното включване на все по-бързо увеличаващия се брой на мобилни абонати, не желаещи да търсят специални точки за включване към мрежата, а глобално погледнато - потребността на съвременния човек от модерни бързодействащи и високоскоростни комуникации [5 , 36, 56, 128, 259, 321].

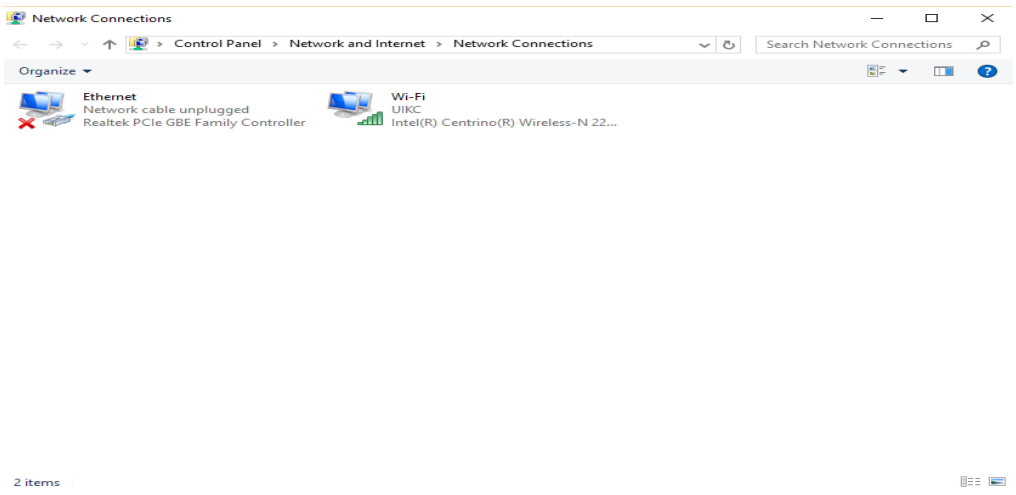
Изграждане на безжични мрежи

[3] https://www.bukvar.bg/materials/browse/11,148,,,,/?page=14&so=1

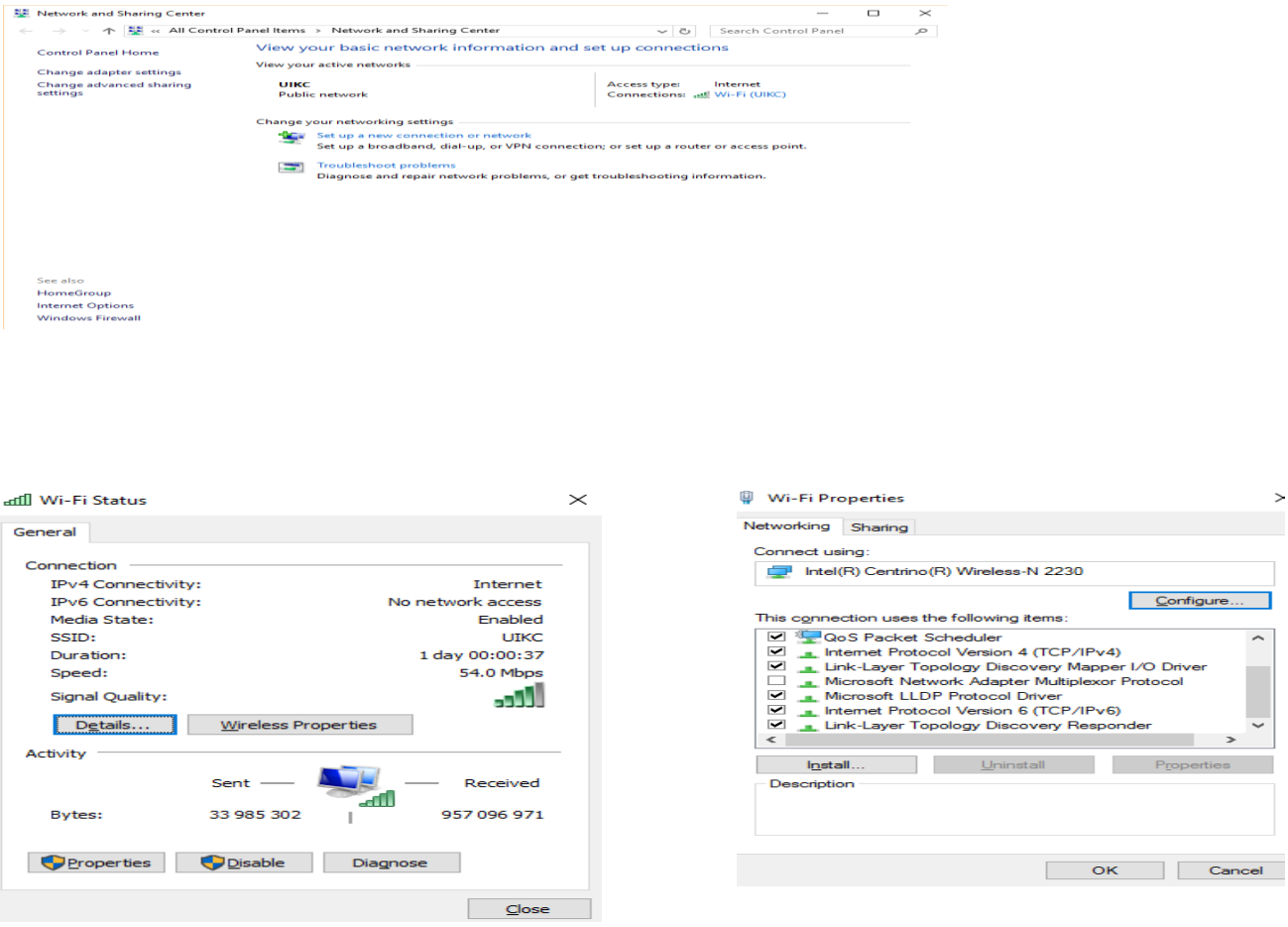
Изграждането на безжични мрежи, изисква определени познания, и то не само по подбора на необходимото оборудване, разполагането му по най-удачния начин, но и по настройването на програмното осигуряване, правата на достъпа и техническата безопасност [45, 59 128 , 149 , 189].

Най-простият начин да се свържат два компютъра в безжична мрежа е да се включи във всеки един от тях по една WLAN карта, без значение с какъв интерфейс е тя (стига да се поддържа), да се инсталират драйвери, да се настроят необходимите параметри на връзка, нива на криптиране, и мрежата е готова да обменя данни между устройствата [5, 69, 128 , 221].

Операционните системи от ново поколение от типа на Windows и Linux [221 -240], след инсталирането на необходимите драйвериразпознават устройствата коректно и позволяват "общуването" с тях, както и настройването на някои параметри[4].



[4] http://pencho.my.contact.bg/start/comp/lan/wlan.htm



Фигура 3 Настройка на безжична мрежа

Безжични комуникационни устройства (WiFi)

WiFi (Wireless Fidelity - в буквален превод “Безжична прецизност”) е вид WLAN - безжична мрежа предназначена за употреба на къси разстояния (до 100 m в закрити пространства и до 300 m на открито), например офиси.

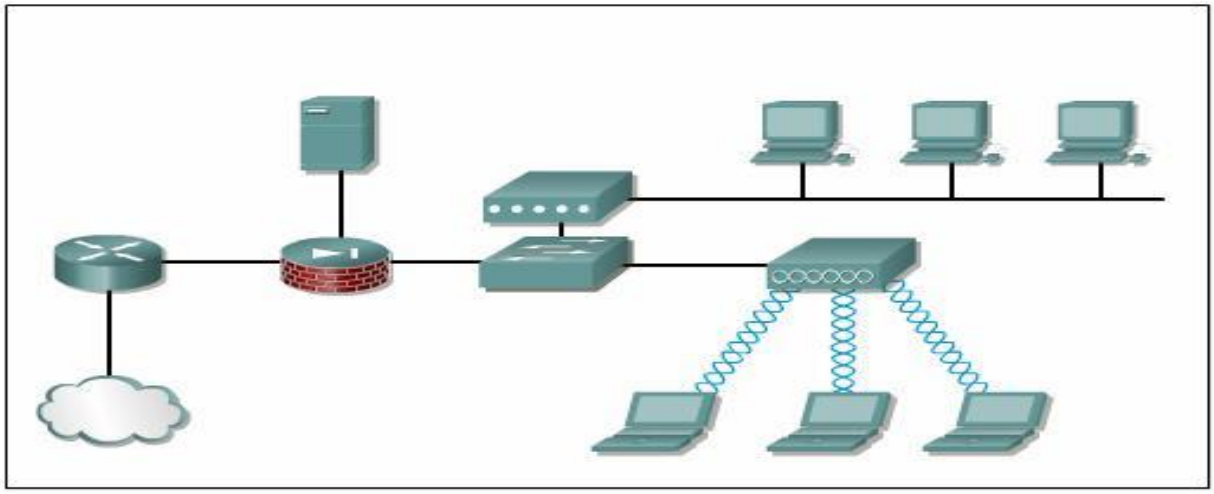
За да може да бъде определена една безжична мрежа като WiFi е необходимо тя да бъде изградена съгласно изискванията на Алианса за съвместимост на безжичните Eternet мрежи (WECA). Спазването на тези изисквания гарантира съвместимостта на безжичните устройства, независимо от това кой е производителят им [25, 58, 258].

Предимства на използването на безжичните устройства WiFi:

- Чрез WiFi се създава едно “гъвкаво” работно място в което може да се работи навсякъде и да се включват нови потребители без добавянето на допълнителни конектори.
- WiFi позволява осъществяване на връзка с интернет навсякъде, където съществува ‘hotspot’.
- Стандарта позволява на офис работниците да използват преносими компютри, чрез които могат да използват мрежата на фирмата от различни местонахождения, което ги прави по- мобилни и гъвкави.

Начин на работа на безжичната мрежа [55, 98, 128, 157]:

Общо казано всяка WiFi безжична мрежа притежава HotSpot (в буквален превод гореща точка”), през който се осъществяват всички връзки в локалната мрежа. Също така той осъществява връзката между безжичната мрежа и други локални мрежи, както и връзката с Internet [159, 168 , 191, 228, 289, 297].



Фигура 4 Безжична система за предаване на данни

Wi-Fi Direct

В скоро време Wi-FiDirect, известен поначало като Wi-FiPeer-to-Peer, ще стане един от основните способи за безжично предаване на данни между устройствата.

Wi-FiDirect – това е нов стандарт за безжично предаване на данни, позволяващо на устройствата да се свързват направо, без допълнително междинно звено във вида на рутер [225, 297, 310].

Понастоящем да се направи направо безжична връзка на принтер към компютър или телефон към лаптоп е невъзможно, за това е необходим още един съединяващ елемент във вида на маршрутизатор.

Wi-FiDirect е разработен, за да бъде отстранено това ограничение и да може да се направи пряка връзка между устройствата.

А дали ще може Wi-FiDirect напълно да измести Bluetooth е трудно сега да се каже със сигурност, но всички предпоставки за това са налице. Спрямо Bluetooth новата производна на Wi-Fi стои доста по-добре както като скорост на предаване и радиус на покритие, така и като защита на данните и простота на свързването.

Избавянето от излишния безжичен интерфейс при мобилните устройства ще е от полза и за производители, и за потребители, защото устройствата стават по-компактни, леки, по-евтини и по-прости за производство. А пък потребителите, вместо да следят два интерфейса, ще го правят за превключването само на един [45, 56, 128, 159].

Новата технология може практически да бъде вградена във всяко едно устройство, в това число и в тези, които традиционно работят с Bluetooth (безжични клавиатури, мишки, слушалки). За увеличаване автономността на Wi-FiDirect са разработени и нови енергоспестяващи режими на работа [158, 198, 197].

Технически характеристики

Втора глава ОБЗОР

Стандарта IEEE 802.15.4/ - ZigBee технологията

ZigBee

ZigBee е една нова технология за безжична връзка, базирана на предаването на данни чрез радио вълни. Това е един изключително гъвкав стандарт покриващ голяма част от нуждите на пазара на безжични устройства. Технологията, също така, запълва една голяма празнина в предлаганите досега продукти. Това е първата технология предлагаща много ниска консумация на енергия, която е от решаващо значение при безжичните устройства [25, 39, 78, 118, 189]

IEEE 802.15.4 стандарта и Zigbee технологията.

IEEE 802.15.4 е стандарт реализиран през май месец 2003г. Той е създаден на базата на прост протоколен стек, като има за цел да осигури хардуерната база за по - нататъчното реализиране на безжични приложения покриващи стандарта.

ZigBee алианса от своя страна е една организация учредена от няколко големи корпорации в областта на високите технологии (Philips, Motorola, Samsung и др.), имаща за цел да направи вече съществуващата технология използваема и да я рентира на пазара [185, 189, 199, 228].

Организацията създава безжична технология базирана на IEEE 802.15.4 стандарта, като добавя към предложените от него възможности и логически мрежови топологии, както и осигурява сигурността на мрежите. Важно е да се отбележи, че ZigBee алианса не налага собствен стандарт, а по-скоро предлага готовнабор от решения, предназначени предимно за сензори и контролни системи [127, 158, 189].

Основни характеристики на ZigBee стандарта

ZigBee технологията има два канала за предаване на данни: 2.4 Ghz и 868/915 Mhz. При 2.4 Ghz честота на канала предаването на данни става с максимална скорост от 250 kbps. При по- нискочестотните канали и скоростта е по-ниска - от 20kbps до 40 kbps [125, 158, 225].

Едно от основните приимущества на ZigBee е ниската консумация на енергия. Едно устройство проектирано на базата на тази технология може да работи с една обикновена батерия от няколко месеца до 2 години, а в някои случай дори повече. Разстоянието на което може да се осъществява връзка е около 50м (типична стойност) (от 5м до 500м в зависимост от средата на разпространение на сигнала). Трансфера на данни се извършва на базата на договаряне (Hand-Shake протоколи).

Друго голямо приимущество на ZigBee е възможността устройствата проектирани на базата на него да изпълняват много различни топологии - звезда (star), от точка до точка (peer-to-peer), всеки с всеки (mesh) и други.

Видове хакерски атаки

WSN можем да ги поделим според някои функции. Някои модели са крайно едноставни: сензора извършва измерване и праща данни. Сложните модели включат изпълнение на сложени алгоритми за работа и обработка на данни. При дискусията за сигурност на WSN требва да изследваме от какво да се защитим а от какво не. Има много форми и видови на атаки[205, 289, 301]. Можем да ги поделим на: Пасивни атаки – за подслушване, наблюдение събиране на данни и т.н., Активни атаки включват фалшива външност (Masquerade), заместване, изменение, отказ на услуги (Denial of service) и т.н. От всичките атаката при която се проявява отказ на услуги е най-опасна, тъй като от останалите може да се защитава

чрез автентификация и криптография. Отказ на услуги представлява опасност за цялата система, което може да се извърши с ненасочена случайна атака, но вероятно е да бъде насочена поради това че в случая е трудно да се определи кой от участниците е и къде е в мрежата. Атаките над WSN можем да ги поделим на няколко групи които следват:

Едноставно събиране (Simple Collection and Tranmittal):

• отказ на услуги – denial of service

• предаване на измислени данни - broadcasting spurious information

• физички атаки – physical attack

• атака с препращане на съобщения – replay attacks

Сензорния възел извършва периодични измервана и ги пращат на базисната станция при предпоставка че е достъпен и е в обсега. Тези типове на WSN е неустойчива на атаки които се отнасят на мрежово ниво [201, 257, 258]. Атаката отказ на услуги (denial-of-service) състои се в блокиране (jamming) или интерференция на радио честоти, което инициира колизия. Също така са усетливи на измамнички (spoofing) атаки в които злонамерения атакува с изпращане на измислени данни (broadcasting spurious information), неустойчиви се на физички атаки (physical attack), както що е откравдване унищожение и т.н. Атаките с повторно изпращане на вече пратено на предишно изготвено съобщение (replay attack) са присъни тук [16. 189, 190, 205].

Препращане (Forwarding):

• черна дупка - Black Hole

• селективно препращане – Selective Forwarding

• корумпиране на данните – Data Corruption

• изтощаване на ресурсите - Resource Exhaustion

Сензора ги събира и ги праща данните на един от съседните сензори които се намира на пътя до базисната станция. Така посредничките сензори ги препращат съобщенията до базисната станция или до съседен сензор така че на край данните да стигнат до базисния сензор. При приемането на данни сензора (в първия случай) не ги обработва само ги предава нататък [15, 85, 94, 172]. Поради това WSN е неустойчива на атаката Black Hole, корумпиране на данните (Data Corruption) и изтощение на ресурсите (Resource Exhaustion). В атаката Black Hole възела които е отговорен за препращане на данните той ги отбива (унищожава). Атаката с корумпиране на данни я променя съдържанието на данните при предаване [187, 186, 275]. Цел на тези атаки е превземане контрол над мрежата. Изтощение на ресурсите се осъществява на този начин че злонамерения праща голямо количество на данни кое представлява излишно трошене на енергийните ресурси (батерията) [185, 189, 205]. Когато пакета има експлицитно зададен път които требва да го помине това се нарича селективно препращане (Selective Forwarding). Получаване и обработка на команди (Receive and Process Commands) [211, 267, 287]:

• пращане на измислени (фалшиви) команди Сензорния възел приема команди от базисната станция която управлява пряко или през техен съсед (непряко) друг възел, при що се пращат команди за променя на състояние или действия. Възможността за обработка на командите е от голяма полза за намаляване на количеството данни в WSN. Командите могат да се пращат към всички възли (broadcast) или към един (unicast). При пращане към един възел нужно е да се осигури някакво адресиране на възлите. Тук идва атаката при която злонамерения възел се заема свойство на главен възел (базисна станция) и изпраща измислени (фалшиви) команди. Само организация (Self-Organisation) [15, 186, 211, 257]:

//atacks aginst routing protocol:

• spoofed, altered, or replayed routing information

• sinkhole attacks

• Sybil attacks

• wormholes

• HELLO flood attacks

• acknowledgement spoofing

Изпълнението на WSN се представлява като само организационна единица коя се учи и управлява с топологията. Информацията за топология на мрежата може да бъде позната само на базисната станция или да бъде споделена с някои друг второ степен главен възелили пак с всички възли в мрежата [14, 52, 185, 199]. От възлите тогава се изиска да се отнасят като клъстери (cluster) за да могат да го решат проблема с колизията в мрежата. WSN, на кратко казано е чувствителна на всички атаки които се отнасят на маршрутните протоколи (routing protocols) [158, 186, 194], тук ще ги споменем атаките Induced Routing Loops, Sinkholes, Wormholes, HELLO Flooding. Когато могат да се преследват данните в самата структура на мрежата, злонамерения може да го променя данните, наново да ги праща същите или да измисли (spoofed, altered, or replayed routing information) [158, 856, 197]. Това я загрозява истинската фигура на мрежата каква я вижда базисната станция.

Трета глава

ЦЕЛИ И ЗАДАЧИ

Целта на този дисертационен труд е да се изследва и анализира предаването на данни в различни компютърни мрежи. Предаването и приемането на данни (или в по-широк план предаването на данни или цифровата комуникация) е предаването и приемането на данни (цифров бит поток или цифровизиран аналогов сигнал над комуникацията от точка до точка или точка до точка. комуникационния канал [58].

Аналоговото или аналоговото предаване е метод за предаване на гласова, данни, изображение, сигнал или видео информация с помощта на непрекъснат сигнал, който варира по амплитуда, фаза или някакво друго свойство пропорционално на параметрите на променливата. Съобщенията се представят или от последователност от импулси, използващи линеен код (предаване в основната честотна лента), или от ограничен набор от непрекъснато променящи се сигнали (предаване с честотна лента) с помощта на метода на цифрова модулация. Модулацията на честотната лента и съответната демодулация (известна още като откриване) се извършва от хардуера на модема. Според най-често срещаното определение за цифров сигнал, както сигналите за базова лента, така и сигналите за честотната лента, представляващи бит потоците, се считат за цифрово предаване, докато алтернативно определение счита само сигнал за базова лента като цифров, така и предаването на цифрови данни в честотната лента като форма на цифрово преобразуване към цифрово. - Аналогово преобразуване.

Данните, които се предават, могат да бъдат цифрови съобщения, произхождащи от източник на данни, например компютър или клавиатура. Също така може да бъде аналогов сигнал, като телефонен разговор или видео сигнал, дигитализиран в bitstream, например с помощта на модулация на импулсен код (CMS) или по-усъвършенствана изходно кодиране (аналогово-към-цифрово преобразуване и компресиране на данни) верига. Това оригинално кодиране и декодиране се извършва с помощта на хардуера на кодека.

От направения анализ можем да направим формулираме следните цели в настоящия дисертационен труд:

1. Да се направи систематичен анализ на различните видове компютърни мрежи и да се анализира сигурността на предаване на данни в тях.
2. Да се разработят математически модели за анализ на информационна система и те да се приложат за различни компютърни мрежи.
3. Да се разгледат различните хакерски атаки и начини за тяхното противопоставяне.

От направените цели могат да се формулират следните задачи

1. Концептуален анализ на методите и подходите за анализ на компютърни мрежи и софтуерни системи

2. Преглед на различните видове протоколи и описание на техните различия – обзор по темата.

3. Разработване на различни софтуерни симулации като се използват различни протоколи и да се анализира преноса на данни и някои характеристики на компютърната мрежа като стабилност на данните, честотна лента и др.

4. Приложение на нова математически подходи за анализ и прогнозиране на стабилността на компютърна мрежи и информационната система в частност.

5. Тестване на компютърни симулации и реализиране на хакерска атака като се анализират различни начини на ентропия и сложността на проведената атака

Дискусия

Настоящите изследвания на мрежовия дизайн от следващо поколение подчертават предизвикателствата, които трябва да бъдат преодолени преди приложения и услуги, които изискват висок капацитет, ниска латентност и подобрена надеждност, могат да се превърнат в норма. Транспортните мрежи имат жизненоважна роля за предоставянето на нови и иновативни приложения и услуги, които напълно използват мрежовите архитектури от следващо поколение. Новата софтуерно дефинирана мрежа (SDN) [25, 33, 35, 44-50] е успешно използвана за подобряване на мрежовите решения, например център за данни и корпоративни мрежи, а текущите изследвания са фокусирани върху по-широкото прилагане на SDN-базирана мрежа към ядрото на оператора и мрежите за достъп, включително безжично мобилно обратно предаване.

Появи се парадигмата за софтуерно дефинирана мрежа (SDN).

през последното десетилетие и сега е готов да бъде напълно адаптиран към транспортни мрежи. Постоянно се разработват нови технологии, които подобряват производителността, надеждността и устойчивостта въведена, за да отговори на бързия растеж в използването на данни и изискването за ниска латентност и подобрена надеждност.

Следващото поколение клетъчни мрежи, включително 5-то поколение (5G) мобилни клетъчни комуникации, ще въведе подобрено качество на преноса на данни. Резултати от опит (QoE) и качество на услугата (QoS), които целят да отговарят на очакванията на потребителите и доставчиците на услуги. Следващото поколение клетъчни мрежи се разглеждат като благоприятните фактори за мрежовото общество, където са повсеместни [43, 66, 161]. Ще бъдат достъпни високоскоростни връзки за данни за

свързване на потребителите и устройства към мрежата. Растежът на комуникациите от машина към машина и очакваното добавяне на стотици, милиони устройства доведоха до появата на термина Интернет на нещата (IoT) [239]. Приет, за да подчертае растежа и промените, които трябва да настъпят като се въвеждат клетъчни мрежи от следващо поколение.

Изследване и развитие на нови технологии и системи за мрежата за радио достъп (RAN) въведе транспортна мрежа свързани предизвикателства, които трябва да бъдат преодолени, за да се гарантира, че следващото клетъчните мрежи за поколение работят според очакванията и улесняват растежа [25, 132, 164] в нови и иновативни приложения и услуги. С клетъчни мрежи от по-ранно поколение може би е било възможно, в някои обстоятелства, до прекомерно осигуряване на транспортната мрежа, като по този начин премахваме необходимостта от сложен дизайн на транспортната мрежа и използването на технологии, които подобряват работата на транспортните мрежи. Прекомерното обезпечаване на транспортната мрежа гарантира това не се превръща в пречка между ядрото и RAN, обаче общата цена на собственост за транспортните мрежи се е увеличила като клетъчни мрежите се разшириха, което доведе до приемане на намаляване на разходите стратегии. Въвеждането на малки клетки, пико клетки и ултра-плътни малки клетъчни мрежи (UDN) [86, 100, 112] създадоха архитектурни, предизвикателства за осигуряване и оптимизиране за бъдеща транспортна мрежа проекти [111-118].

Тествана на компютърна система с Raspberry PI по метода на грубата сила

Описание на алгоритъма

1. Въведение

Целта на този текст е да покаже нагледно как мини компютъра Raspberry Pie 3 може да се изпозлва за WIFI хакване. (може да добавиш кратки технически спецификации за устройството).

2. Нужен Хардуер / Нужни Компоненти

- Raspberry Pie 3

- Micro SD карта (16GB)

- Четец за картата (USB Micro SD Card Reader) - използва се за да копираме обновения фърмуер от нашия компютър.

- Ethernet кабел - Използва се за връзка между Raspberry Pie 3 и WIFI рутер. Нужен е, за да може да контролираме Raspberry Pie 3 от друго устройство, което също е свързано с рутера.

- Адаптер (2.5 Ампера) - захранване

3. Инсталиране на Фърмуера

Попринцип, режима на проверка (monitor mode) на Raspberry Pie 3 не работи. За да можем да го използваме, трябва първо да исталираме обновения фърмуер.

Можем да обновим фърмуера както следва:

- Сваляме фърмуера на нашия компютър

- Слагаме/Включваме Micro SD картата в слот-а

- Извличаме (Extract) сваления файл с Winrar (Windows) или Unarchiver (Mac)

3.1 Инсталация в Windows

Първо трябва да инсталираме Win32 Disc Imager. След това отваряме програмата, маркираме извлечения/ разархивирания файл и натискаме write.

Не е лошо да има скриин шот тука или по-точно изрязано само прозореца на програмата с snipping tool като в клипчето

3.2 Инсталация в MAC

Първо отваряме терминал, в който пишем **discutil list.** Чрез тази команда идентифицираме кой диск е нашата SD карта. След това използваме командата

diskutill unmountDisks Disk1 (като Disk1 в случая е SD картата ни**).**

Продължаваме с **Sudo dd bs=1m if [**пътеката към имидж-а] of=/dev/rdisk1(като Disk1 в случая е SD картата ни). След това изчакваме командата да се изпълни.

Следващата стъпка е да включим SD картата в Raspberry Pie 3. След това свързваме устройството с рутера, чрез Ethernet кабела. Последната стъпка, за да е вкючено и свързано всичко е да пуснем и захранващия адаптер.

4. Как да намерим IP адреса на Raspberry Pie 3

За да можем да управляваме Raspberry Pie 3, трябва да знаем локалния IP адрес на устройстовто. Има много различни методи да намерим адреса му. Предложените методи използват софтуер за сканиране на IP адреси, като в случая използваме Angry IP Scanner.

След като намерим IP адреса на Raspberry Pie 3, вече можем да го контролираме.

5. Контролиране на Raspberry Pie 3 (Windows и Mac)

Windows

Първо трябва да свалим допълнителен софтуер, в случая Putty.

След зареждане на апликацията, въвеждаме IP адреса на Raspberry Pie 3.

Вписваме се като **Root (Login as: Root)**

Въвеждаме паролата, която по подразбиране е **toor.**

MAC

Отваряме терминал и въвеждаме следното: **ssh root@192.168.1.113** [адреса е примерен - трябва да се въведе IP адреса на Raspberry Pie 3].

Вече всичко е конфигурирано и работи и можем да започваме хакването.

*Можем също да използваме terminal emulator, за да установим ssh връзка през нашия Android смартфон.

6. WIFI Хакване

Трябва да изпълним определени стъпки както следва, за да завършим WIFI хакването успешно.

1. Намиране файл-а, който съръжа паролата за WIFI мрежата (*.cap)

2. Копиране на списък с пароли на Raspberry Pie 3 чрез ÙSB.

3. Изпълняване na wordlist атака срещу .cap файл-а

6.1 Намиране /Улавяне (capture) файл-а, който съръжа паролата за WIFI мрежата (*.cap)

Отваряме връзката с терминала на Raspberry Pie 3. Пишем командата **monstart**, за да пуснем режима на проверка на мрежовата карта, след което въвеждаме **airodump-ng wlan0**, за да видим всички рутери в обсег.

За целта на този текст ще приемем, че мрежата на рутера който хакваме се казва **Wireless Network**. Щом идентифицираме мрежата, която търсим трябва да уловим (capture) handshake файл-а, който съдържа паролата за WIFI мрежата на рутера.

За да изпълним тази задача, трябва да запишем номера на канала (№6 в нашия случай, както и BSSID.

Натискаме ctrl +C, за да спрем процеса и да се върнем в полето за команди (command line). След това въвеждаме следното:

Компютъни симулации на различни протоколи със софтуерния пакет Matlab

Една мрежа може да бъде организирана по два начина:

като равноправна (peer to peer) работна група, в която всеки компютър може да изпълнява ролята на клиент или на сървър, при което всеки един от потребителите самостоятелно администрира ресурсите на своя компютър;

като сървърно-базирана мрежа, администрирането на която е съсредоточено в един централен компютър, наричан сървър.

Равноправните мрежи са подходящи за малки мрежи, включващи не повече от 10 компютъра. Всички компютри в една такава мрежа образуват една обща работна група (workgroup). Това изисква всеки един от компютрите да бъде конфигуриран за работа в работна група. В Windows това се извършва чрез съответна настройка на компютъра за работа в мрежа, като името на работната група трябва да бъде едно и също за всеки един от компютрите.

В сървърно-базираните мрежи достъпът до ресурсите бива контролиран посредством *автентикация* (*authentication*) и *разрешения* (*permissions*). За всеки споделян ресурс мрежовият администратор задава разрешения (права на достъп) за всеки отделен потребител или за цяла работна група. Чрез разрешенията се указват нивата на достъп до ресурсите, например дали даден файл може само да бъде прочитан или в него могат да бъдат извършвани и промени (редакция или изтриване) [7-10].

В тази нова информационна ера, високите скорости на данни и високата надеждност тласкат нашите безжични системи напред и се превръщат в доминиращ фактор за успешното разгръщане на търговски мрежи. MIMO-OFDM (мултиплексиране с множество входове и ортогонално честотно разделяне), нова безжична широколентова

технология, придоби голяма популярност поради възможностите си за високоскоростно предаване и надеждността си срещу многоканално затихване и други канални смущения. Основното предизвикателство за MIMO-OFDM системите е как точно и бързо да се получи информация за състоянието на канала за последователно откриване на информационни символи и синхронизация на канала. В първата част на работа е формулиран проблем за оценка на канала за MIMO-OFDM системи и е предложен алгоритъм за оценка, базиран на пилотен тон.

Сложен еквивалентен модел на MIMO-OFDM сигнали с основна лента е представен чрез матрично представяне. Чрез избиране на еднакво разположени и еднакво мощни пилотни тонове от подносещите в един OFDM символ, се получава намалена дискретна версия на оригиналния модел на сигнала. В допълнение, този модел на сигнала се преобразува в линейна форма, която е разрешима за алгоритъма за оценка на LS (най-малък квадрат). Въз основа на получения модел се предлага прост дизайн на пилотни тонове под формата на единна матрица, чиито редове представляват различни набори от пилотни тонове в честотната област, а колоните на която представляват различни предавателни антени в пространствената област. От анализа и синтеза на дизайна на пилотния тон в тази разработка, нашият алгоритъм за оценяване може да намали изчислителната сложност, наследена в MIMO системите от факта, че матрицата на пилотния тон е по същество единна матрица и е доказано, че е оптималният оценител на канала в смисъл на постигане на минимум.

MSE (средна квадратична грешка) оценки на канала за фиксирана мощност на пилотния тон. Втората част на тази дисертация разглежда проблема с безжичното местоположение в WiMax (глобална съвместимост за микровълнов достъп) мрежи, която се базира основно на MIMO-OFDM технология. От измервателните данни TDOA (Разлика във времето на

пристигане), AOA (Ъгъл на пристигане) или комбинация от двете, се формулира квазилинейна форма за решение от тип LS. Приема се, че данните от наблюдения са изкривени от нулева средна AWGN (адитивен бял гаусов шум) с много малка дисперсия. Съгласно това предположение се доказва, че терминът шум в квазилинейна форма има приблизително нормално разпределение. Следователно оценката на ML (максимална вероятност) и решението от типа LS са еквивалентни. Но техниката за оценка на ML е неприложима тук поради нейната изчислителна сложност и възможното отсъствие на оптимално решение.

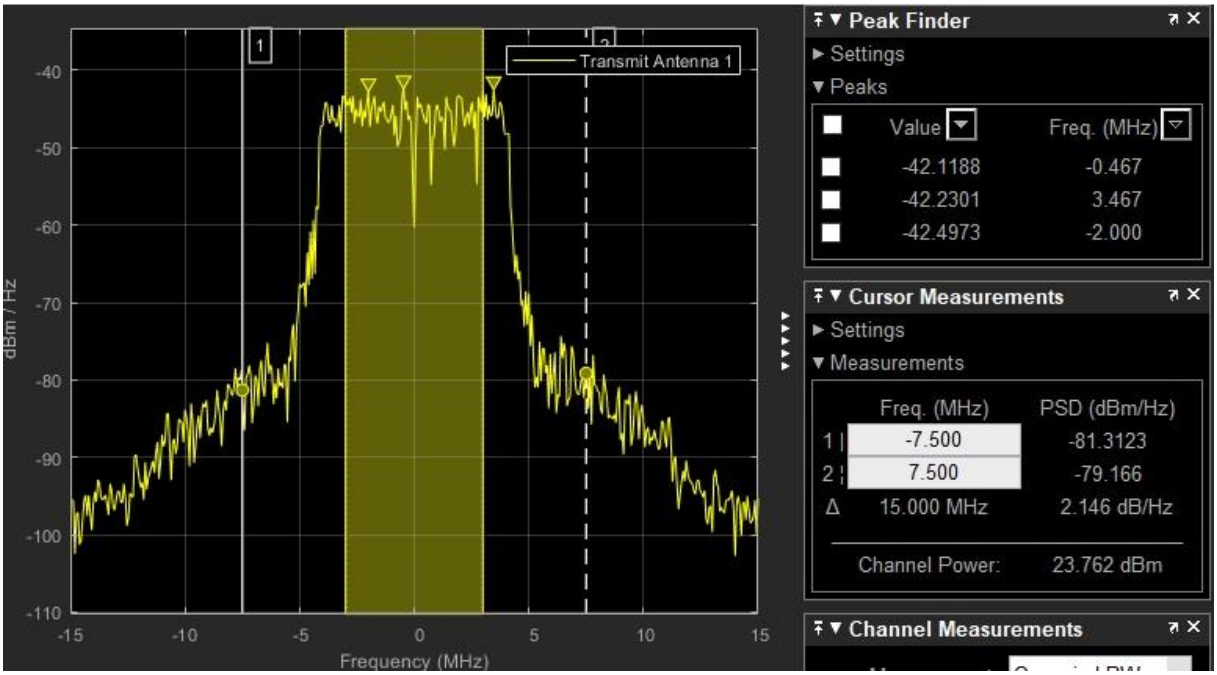
IMO-OFDM системите са норма в съвременните безжични системи (напр. 5G NR, LTE, WLAN) поради тяхната надеждност за честотно селективни канали и висока скорост на данни. С постоянно нарастващите изисквания за поддържани скорости на данни, тези системи стават все по-сложни и големи в конфигурации с нарастващ брой антенни елементи и специални ресурси (подносещи).

С антенни решетки и пространствено мултиплексиране са необходими ефективни техники за предаване [6]. Формирането на лъч е една такава техника, която се използва за подобряване на съотношението сигнал/шум (SNR), което в крайна сметка подобрява производителността на системата, измерена тук по отношение на честотата на битовата грешка (BER) [1].

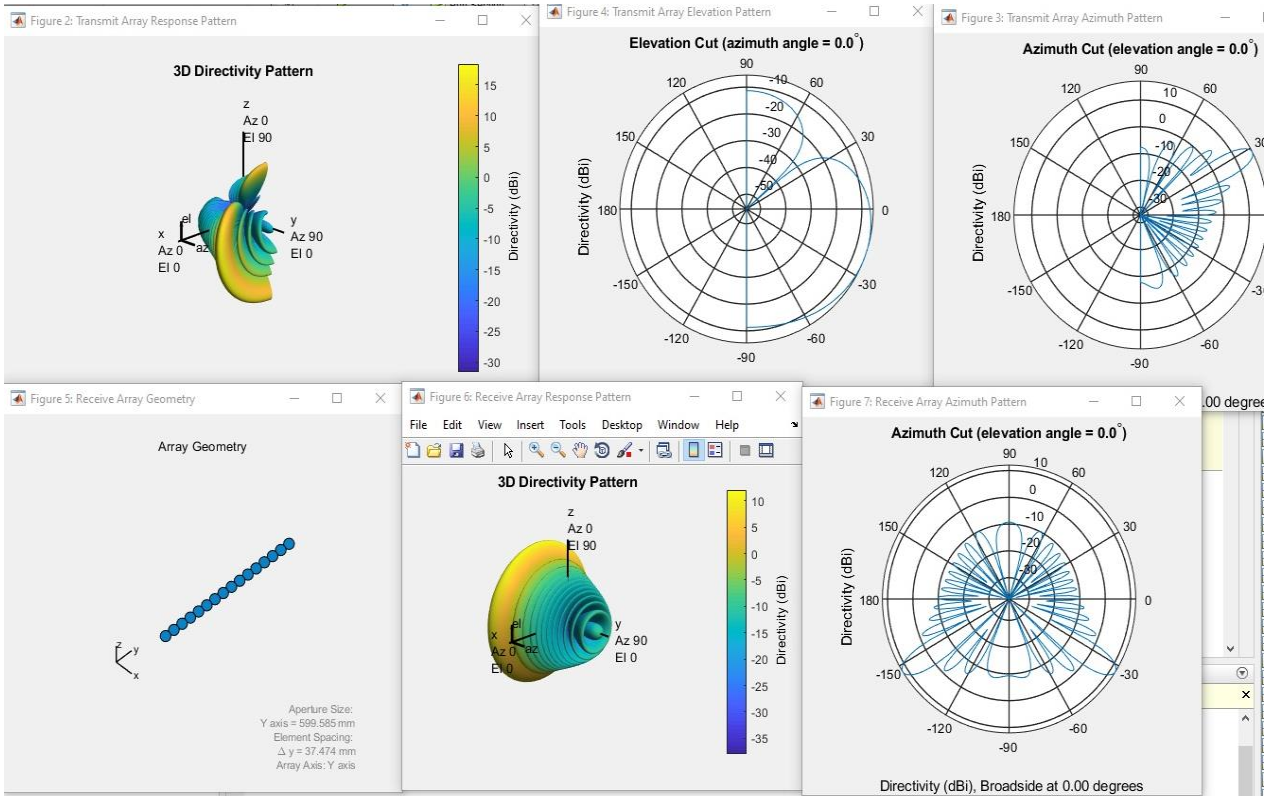
Този пример илюстрира асиметрична еднопотребителска MIMO-OFDM система, където максималният брой антенни елементи в предавателния и приемния край може да бъде съответно 1024 и 32 с 16 независими потока данни. Той симулира пространствен канал, където местоположенията на масива и моделите на антените са включени в цялостния дизайн на системата. За простота се моделира единична комуникация от точка до точка (една базова станция, взаимодействаща с

един мобилен потребител). Каналът използва звучене на канала, за да предостави на предавателя информацията за канала, необходима за формиране на лъч.

Примерът предлага избор от няколко пространствено дефинирани канални модела, по-специално модела на канала WINNER II и модела на базата на разсейване, като и двата отчитат пространствените местоположения на предаване/приемане и моделите на антената (Фиг. 27 и 28).

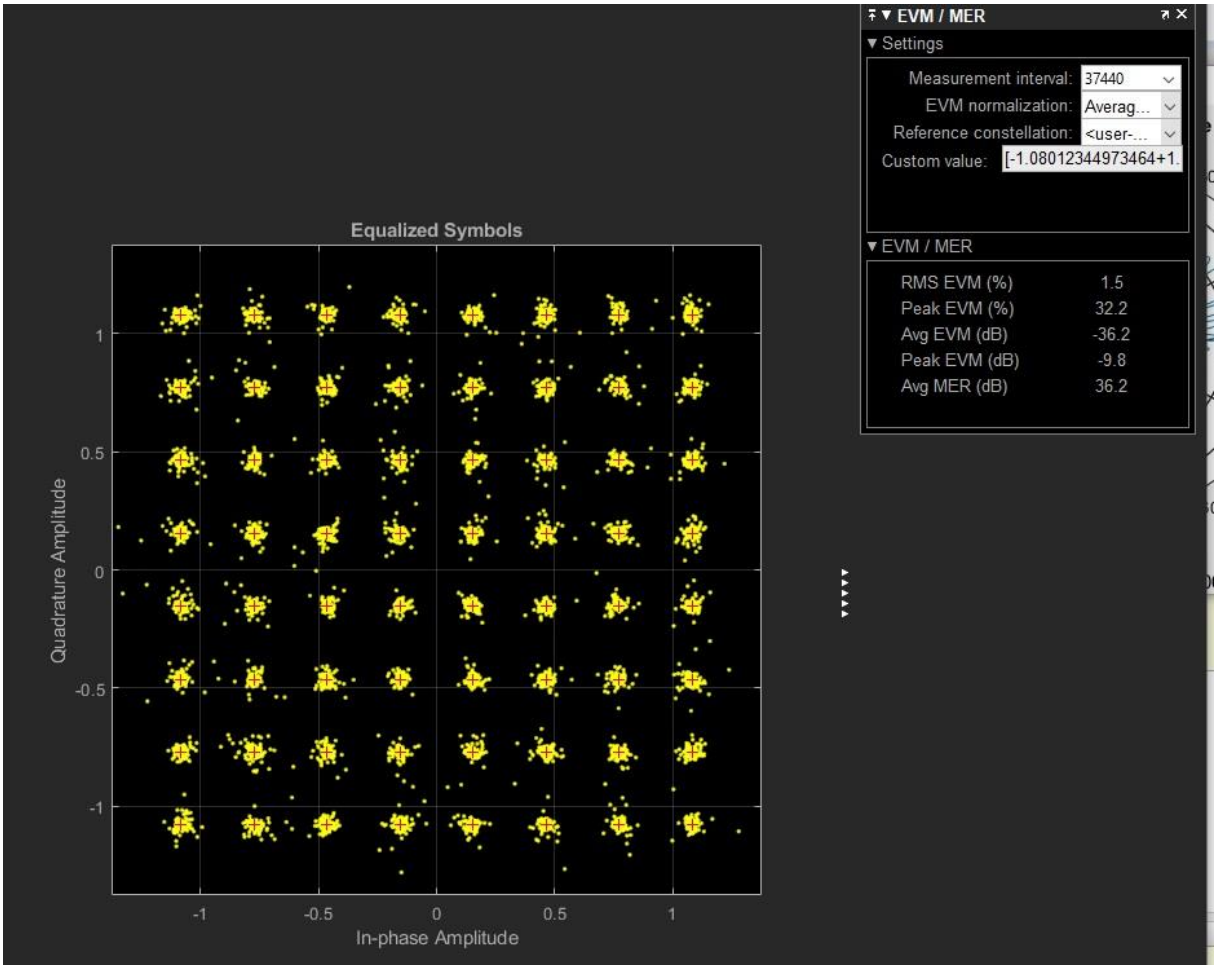


Фигура 5 Анализ на честотната лента на компютърна мрежа с matlab



Фигура 6 Симулация на предаване на данни и анализ на шумове с matlab 2018 работа с пакет MIMO-OFDM Precoding with Phased Arrays[5]

5 Perahia, Eldad, and Robert Stacey. Next Generation Wireless LANS: % 802.11n and 802.11ac. Cambridge University Press, 2013.



Фигура 7 Разсейване на шумовете - matlab 2018 работа с пакет MIMO-OFDM Precoding with Phased Arrays

МАТЕМАТИЧЕСКИ МОДЕЛИ ЗА АНАЛИЗ НА КОМПЮТЪРНА СИСТЕМА

Теория на игрите

В теория на игрите противниците се наричат играчи. Всеки от тях има множество от възможни ходове. То може да бъде крайно или безкрайно. Възможните действия се наричат стратегия на играта. Резултатите или плащанията се дефинират от функции, зависещи от стратегията на играча.

Матрична игра на двама играчи е такава игра с нулева сума е такава, при която сумата от печалбите на първия и втория играч ν_1 и ν_2 е равна на нула:

$\nu_1 + \nu_2 = 0.$

Ако първият и вторият играч изберат съответно смесена стратегия x= ($x_1, x_2, \ldots x_m$) за y= ($y_1, y_2, \ldots y_m$), то математическото очакване за печалба на първия играч е

$$E(x,y) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} x_i y_j$$

Нека X и Y са множествата от смесени стратегии на x и y.

Възниква въпроса за съществуване на оптимална стратегия x^* и y^* за печалба (загуба) на първия, респективно втория т.е. математическото очакване за първия е максимална печалба (съответно загуба) е максимално при най-добра игра на противника.

Според основната теорема от теория на игрите съществуват оптимални стратегии x^* и y^* т.е. за матрична игра с нулева сума има решение

$$\max_{x\in X}\min_{y\in y} E(x,y) = \min_{y\in y}\max_{x\in X} E(x,y) = E(x^*,y^*) = \upsilon$$

Така че за всяко $x \in X$ и $y \in Y$ е изпълнено

$E(x^*,y) \le E(x^*,y^*) \le E(x,y^*)$

Числото $\upsilon = E(x^*,y^*)$ се нарича цена на играта, а точката в която се постига се нарича седлова точка[6].

[6] Vladimir Mazalov Mathematical Game Theory and Applications, Wiley, 2012, ISBN 978-1-118-89962-5

Ако интерпелираме представените резултати ако имаме двама играчи в една кибер система единия се отбранява, другия атакува винаги съществува оптимална стратегия за защита, респективно атака[7].

t=0

Нека да разгледаме и друга стратегия L играчи (хакери) атакуват, N/L са атакуемите компютри – вторите играчи.

Използвайки модела на Hamilton–Jacobi–Bellman

$$\widehat{V}_L(x) = \max_{u_i \in L} \lim \left\{ \sum_{i \in L} \log u_i + \varepsilon \widehat{V}_L \left(\varepsilon x - \sum_{i \in L} u_i - \sum_{i \in N \setminus L} \widehat{u}_i \right)^{\alpha} \right\}$$

$$\widehat{V}_L(x) = \max_{\widehat{u}_i \in N \setminus L} \lim \left\{ \sum_{i \in L} \log \widehat{u}_i + \varepsilon \widehat{V}_L \left(\varepsilon x - \sum_{i \in L} u_i - \sum_{i \in N \setminus L} \widehat{u}_i \right)^{\alpha} \right\}$$

Търсене на решение в следната форма

$$\widehat{V}_L(x) = \widehat{A}_L \log x + \widehat{B}_L \text{ , } \quad \widehat{V}_i(x) = \widehat{A}_i \log x + \widehat{B}_i$$

Контрола на потока може да се дефинира по следния начин $u_i = y_i^K x, i \in L$, $\widehat{u}_i = \widehat{y}_i^K x$.

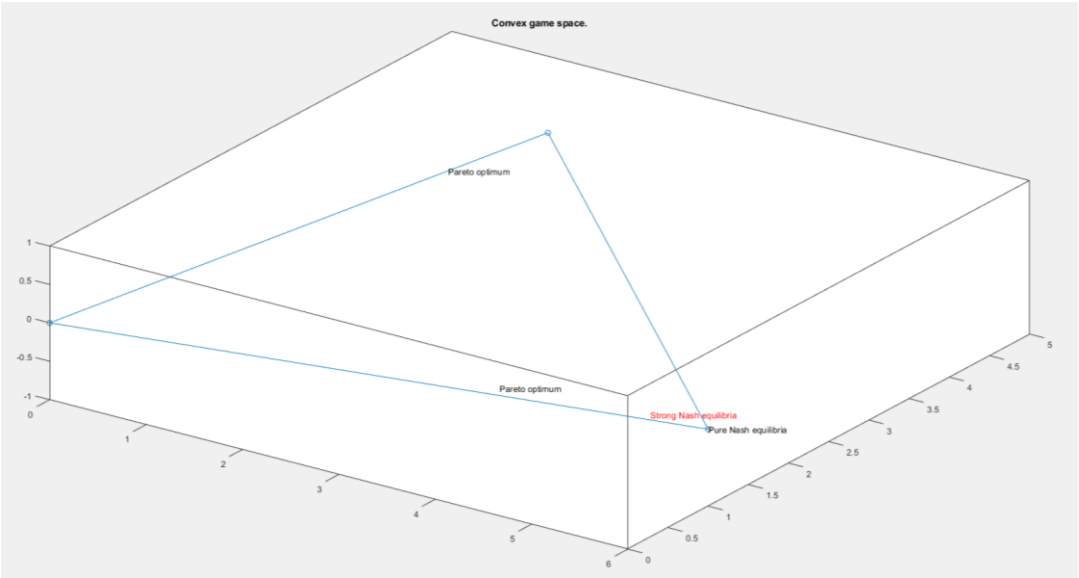
За оптимално решение получаваме следните коефициенти

$$V_i^k = \frac{1-a}{k(1+(n-k)(1-a))} \delta x$$

$$\widehat{V}_L(x) = \frac{k}{1-a} \log x - \frac{1}{1-\delta} \widehat{B}_L .$$

$$B_L = k \left(\frac{1}{1-a} \log \left(\frac{\delta}{1+(n-k)(1-a)} \right) + \log(1-a) + \frac{a}{1-a} \log(a) - \log(k) \right)$$

7 Vito (2021). Game Theory (https://www.mathworks.com/matlabcentral/fileexchange/51601-game-theory), MATLAB Central File Exchange. Retrieved November 10, 2021



Фигура 8 Решение на матрична игра в смисъла на Парето

Приноси

Въз основа на извършените изследвания и анализи дисертацията предлага следните научно-приложни приноси:

1. Откроени са проблемни области в областта на обмен на информацията при различни компютърни мрежи и е направен систематичен обзор.

2. Представени са различните методи хакерски атаки и методи на тяхната защита тази група атаки включва всеки опит за получаване на неоторизиран достъп до системата. Направен е анализ на различните видове атаки като:

    - Атаки от тип „отказ от услуга“ (DoS): вид атака, която причинява загуба на услуга или невъзможност на мрежата да функционира.
    - • Уеб атаки: това е всяка атака, която се опитва да наруши/промени даден уеб сайт. Две от най-често срещаните такива атаки са: SQL injection (SQLi).
    - • “Отвличане” на HTTP сесии (Session hijacking): тези атаки представляват отвличане на идентификатора на потребителската сесия (session hijacking).
    - • DNS отравяне (DNS poisoning): този тип атаки компрометират DNS сървъра така, че потребителите могат да бъдат пренасочени към зловредни уеб сайтове.

3. Разработен е метод на хакерска атака по метода на грубата сила. Реализиранd с хириден компютър от типа Ардуино. Направен е анализ на сложността на атаката.

4. Разработени са математически модели за анализ на стабилността на сигурността на компютърна мрежа и начини за анали на тази система. Използвани са математически подходи като Марковски процеси, Теория на игрите с природата с приложение на принципа на Белман и Теория на катастрофите.

5. В софтуерния пакет Матлаб са направени множество симулации за анализ на преноса на данни в различни компютърни мрежи и влиянието на шума върху този пренос.

6. Анализиран е трафика на компютърна мрежа на интернет доставчик и са систематизирани основните атаки извършвани върху доставчика.

7. Направен е концептуален анализ на видовете компютърни атаки и начините им на провеждане върху бюджетните предприятия.

Заключение

Темата за мрежите, дори и само безжичните мрежи, е наистина огромна и не може да бъде обхванатa само в една разработка. Надявам се, че с този материал съм Ви дал някоя начална информация и съм ви ориентирал по отношение на това, какво точно представлява т най-разпространените за момента безжични технологии и техните протоколи за достъп.

Сравнявайки двата типа комуникации - жичните и безжичните, могат да се видят значително повече предимства при безжичните, отколкото недостатъци, дори и в сравнение с Ethernet. Безспорно, технологиите ще продължават да се развиват с все още по-нарастващо темпо, изчиствайки грешките и неточностите, увеличавайки скоростите за обмен и грижейкисе по-добре за съхраняването на ценните ни данни.

Протоколите за достъп до съобщителната среда при безжичните локални мрежи се различават от протоколите за множествен достъп при кабелните мрежи поради променящите се във времето параметри на съобщителния канал и явлението скрит терминал.

Използването на общ MAC протокол за ISM радиоканали и дифузен инфрачервен канал води до усложняване на протокола. Действащият в момента 802.11 MAC протокол показва добри резултати предимно при радиоканалите.

Предложена е модификация на протокол за управление на достъпа до съобщителната среда при безжични локални мрежи с дифузен инфрачервен канал,който решава проблема с възможните конфликти при обмена на кадри с данни и наличие на скрити станции от тип H2 вмрежата.

СПИСЪК ПУБЛИКАЦИИ

от Илиян Владимиров Иванов

редовен докторант в катедра „Комуникационна и компютърна техника и технологии ”

при Технически факултет

на ЮЗУ „Неофит Рилски”, гр. Благоевград

Статии

1. Trenchev, I., Stoykov, D., Traykov, M., Stefanov, A., Trencheva, M**., Ivanov, I**., (2020) ***Create 3D models by explicitly describing and moving the virtual camera using EEG Signals***, in proceeding The Future of Education - 10th edition, 18-19 June 2020, ***(Indexed in Web of Science)***

- https://conference.pixel-online.net/FOE/files/foe/ed0010/FP/6778-ICT4765-FP-FOE10.pdf

2. Stefanov, A., **Ivanov, I**., Trenchev, I., Stoev, R., Trencheva, M**.,** (2020), ***Usage of mathematical models for cybersecurity analysis*** in proceeding The Future of Education - 10th edition, 18-19 June 2020, ***(Indexed in Web of Science)***

- https://conference.pixel-online.net/FOE/files/foe/ed0010/FP/6778-HED4764-FP-FOE10.pdf

Доклади в научни форуми (конференции)

1.Иванов, И., (2021), „***Изследване на локални мрежи със софтуери*** “, Девети национален семинар на тема „Интелектуалната собственост в новото (не) нормално“, стр. 183 – 189, София, 26 април 2021 /под печат/.

2.Иванов, И., (2021), „***Обучението по мултимедийни и облачни технологии*** “, Девети национален семинар на тема „Интелектуалната собственост в новото (не) нормално“, стр. 177 – 182, София, 26 април 2021 /под печат/.

ANALYSIS AND SIMULATION INVESTIGATION OF THE FEATURES OF LOCAL NETWORKS

Wireless computer networks are the result of the natural evolution of computer systems in terms of flexibility in the use of computing resources and the freedom of users available in space and time. Current technological solutions used for wireless data transmission, depending on the geographical location of the user and the distance at which the data is transmitted.

Wireless LAN LAN-WLANs are one of the parts of wireless computer networks that find application for the implementation of computer communications and network applications in the local area of the type "in-root, in-building or campusarea". Their purpose is similar to cable-based LAN - to transfer data frames between mobile or fixed stations belonging to the network, providing the following additional features:

- Expansion of traditional local area networks for mobile devices.
- Mobile access to corporate networks.
- Local area networks with equivalent access of the Ad Cape type.
- Inter-LAN Bridge remote access bridges.
- Integration of computers and communication devices.

When considering the problems and parameters, the leading criteria are to ensure the maximum data transfer rate and determine the probability of errors (BER - bit error rate). However, the practical transmission of data is performed by the protocols realizing the access to the communication environment (MAC - media access control).

The purpose of this study is to review the most common methods of access to the communication environment in WLAN and their corresponding MAC protocols, how to operate and build wireless networks and types of computer networks. In recent years, the development of technology has increased the need for different types of communications [1-6]. One of the fastest growing methods

of communication is wireless. The biggest advantage of wireless communications is the mobility of the devices they use. In recent years, many wireless standards have emerged, the most popular of which are -Bluetooth, IEEE 802.15.4 / ZigBee, WiFi (802.11 *), Wi-Fi Direct. These standards are designed for a wireless connection that requires a medium high and high data rate [5-12]. For the implementation of the present work, the access protocols for wireless local area networks (WirelessLAN-Wlan) and the basic wireless standards are presented, as well as the most common types of microcontrollers. The 802.15.4 / ZigBee standard is also discussed, compared to other wireless standards.

The first chapter describes the general characteristics of computer networks and the topology of different types of networks. The OSI model is briefly reviewed and characteristics at its levels are presented. Particular attention is paid to Wi-Fi and the protocols it uses. The reason for this is that in the third chapter most computer simulations are made with WiFi.

In the second chapter an overview of the topic of the dissertation is made. The IEEE Standard 802.15.4 / - ZigBee is briefly described. This is an extremely flexible new technology that covers much of the needs of today's market. It is characterized by low energy consumption and relatively good security. The main types and characteristics of different types of hacker attacks are presented. An analysis of the quality and quantity of the different types of damage they can do has been made.

The third chapter presents the results of the dissertation. Conditionally, they can be divided into three groups:

- Computer simulations for studying the characteristics of computer protocols with the software package - Matlab;
- Development of mathematical models for analysis of computer security and entropy of protocols and information system;
- Practical testing of computer security in data transmission and analysis of Cyber security of certain software systems.

The chapter describes a practical attack implemented by the method of brute force using Raspberry PI. Analyzes of hacker attacks on real Bulgarian companies are presented.

SOUTHWEST UNIVERSITY “NEOFIT RILSKI”

FACULTY OF ENGINEERING

DEPARTMENT OF COMMUNICATION AND COMPUTER ENGINEERING AND TECHNOLOGIES

Author’s thesis summary

on

DISSERTATION WORK

For awarding an educational and scientific degree

DOCTOR

Doctoral program

Computer systems, complexes and networks

Field of higher education 5. Technical sciences, professional field 5.3.

Communication and computer equipment and technologies

ANALYSIS AND SIMULATION STUDY OF THE FEATURES OF LOCAL NETWORKS

Supervisors: Assoc. Prof. Dr. Alexei Stefanov
Assoc. Prof. Dr. Ivan Trenchev

Doctoral student: Ilian Ivanov

Blagoevgrad, 2021.

I would like to express my great gratitude to ***Assoc. Prof. Dr. Eng. Alexei Stefanov ,*** who extended his hand to me at an extremely difficult time for him. The strength of will, erudition, intellect and pursuit of good that he possessed, the energy he invested in science and engaging the potential of young people, inspired me. It will always be a shining example for me to follow on my path. It will be my duty in the future to pass on this knowledge - to learn, to be able to develop in a shared way - not only for myself, but to give the young of my energy just enough to ignite the flame in them. of the true attraction to science that lasts a lifetime.

I would also like to express my gratitude to ***Assoc. Prof. Ivan Trenchev*** , PhD, who guided me all the time, gave me ideas, courage and opened new horizons for me .

The dissertation works at the Southwestern University "Neofit Rilski" . The dissertation was discussed and directed for defense at an extended meeting of the Department Council of the Department of Communication and Computer Engineering and Technology of the Southwestern University "Neofit Rilski" in April 2022.

The dissertation has a volume of 193 pages. The main text is systematized in three chapters. Outside it are: *Introduction , Conclusion , Contributions to the dissertation research, Reference apparatus, containing: used literature.*

References include 337 sources.

The public defense of the dissertation will take place on April 11, 2022. From ..... hours in the hall .... at SOUTHWEST UNIVERSITY “NEOFIT RILSKI” , 66 Ivan Mihailov Str. Blagoevgrad, 2700

Contents

Introduction

Wireless computer networks are the result of the natural evolution of computer systems in terms of flexibility in the use of computing resources and the freedom of users in space and time. Current technological solutions used for wireless data transmission, depending on the geographical location of the user and the distance at which the data is transmitted.

Wireless LAN LAN - WLAN is one of the parts of wireless computer networks that find application for the implementation of computer communications and network applications in the local area of the type " in-root , in-building or Their purpose is similar to cable-based LANs - to transfer data frames between mobile or fixed stations belonging to the network, providing the following additional features:

- Expansion of traditional local area networks for mobile devices.
- Mobile access to corporate networks.
- Local area networks with equivalent access of the Ad Cape type.
- Inter -LAN Bridge remote access bridges .
- Integration of computers and communication devices.

When considering the problems and parameters, the leading criteria are to ensure the maximum data transfer rate and determine the probability of errors (BER - bit). error rate). However, the practical transmission of data is carried out by the protocols realizing the access to the communication environment (MAC - media access control)

The aim of this study is to review the most common methods of access to the communication environment in WLAN and their corresponding MAC protocols, how to operate and build wireless networks and types of computers networks.In recent years, the development of technology has increased the need for different types of communications [1-6]. One of the most dynamically evolving methods of communication is wireless. The biggest advantage of wireless communications is the mobility of the devices they use. In recent years, many wireless standards have emerged, the most popular of which are - Bluetooth , IEEE 802.15.4 / ZigBee , WiFi (802.11 *), Wi-Fi Direct . These standards are designed for a wireless connection that requires a medium high and high data rate [5-12]. For the implementation of the present work, the access protocols for wireless local area networks (WirelessLAN-Wlan) and the basic wireless standards are presented , as well as the most common types of microcontrollers. The 802.15.4 / ZigBee standard is also discussed, compared to other wireless standards.

Chapter One

Types and characteristics of computer networks

overview

A network is two or more computers connected to each other by the necessary hardware and software that allow them to exchange information with each other and between other devices. The hardware connection between the individual computers and the other peripherals involved in the network can be built with the help of cables (coaxial, twisted pair, optical), or with the help of some wireless technology (IRDA, Bluetooth). Many network protocols (TCP / IP, NetBEUI , AppleTalk , PPTR, DHCP) take care of the network connection [12]. Generally speaking, there are two types of network - LAN Area Network (local area network) and WAN (Wide Area) Network - network over a wide area). A LAN is a network between multiple computers and peripherals, physically located in a sufficiently small area — for example, within one or more adjacent buildings [28].

WAN is a network that can extend a huge distance, and its main purpose is to connect existing LANs in one network. In turn, one WAN can be connected to another WAN, forming a higher level in the network hierarchy.

The best example of a WAN is the Internet. The data transfer rate between two network devices is one of the most important indicators characterizing the network and is measured in the number of bits transmitted per second [18-29]. In sync with the increasing data rates there were abbreviations such as Kbps , Mbps , Gbps , meaning thousands, millions and billions of bits per second. In terms of LAN design, you can find many terms, the main ones being:

- network type - network with equal access and client - server type

- topology - bus, circular and star
- architecture - Ethernet , TokenRing

Types of networks

In today's world of computer technology, the connection between the computer and external devices is needed, as well as with other computers and computer networks. There are several types of connections. They can be wired or wireless. Each personal computer is usually equipped with two serial and one parallel port. Serial and parallel interfaces work differently The connection between electronic devices can be made in two ways. It is possible to use cables as a transmission medium or wireless technology.

Wired interfaces are mainly used in desktops. But with the advent of laptops and smart mobile phones, wireless standards for data transmission are evolving [18, 28-42].

Classification according to the method of transmission:

Serial

Serial ports send one bit across the transmission medium. Although bit - by - bit transmission is required on the transmission medium, the number of wires is significantly smaller.

There are two main types of serial communications - synchronous and asynchronous [28, 35, 78].

Synchronous interfaces exchange information about synchronization before the start of the transfer, but also exchange synchronization signals during it [28, 31-38]. Synchronous transfers allow a higher exchange rate than asynchronous ones.

Asynchronous communication means one in which there is no synchronization [45- 62]. No "empty" bits are sent. The serial port of personal computers is asynchronous. Although there is no synchronization, the beginning

and end of each byte transmitted must be indicated. This is done by starting and stopping bits.

Parallel

Parallel ports send and receive information by transmitting 8 bits of data simultaneously on a cable consisting of 8 wires. This method allows very fast communication, but the cable used is inconvenient because it is thicker and composed of many wires. Parallel ports are mostly used to connect a computer to a printer.

Classification according to the rights of connected computers

There are two basic types of local area networks, which differ in what rights the connected computers have and how they receive them. In a network with equal access, each computer has equal rights, while in a client-server network it is the server that determines the access rights to other participants in the network at the request of each client computer. Incidentally, a local area network can be a combination of the two types [25, 78-91].

Equal access network.

As the name implies this type of network, all participants in the vagueness are equal, and at one time a computer can act as a server, and at another - as a client. Access to shared network resources is administered by a separate server, as is the case with client-server networks. This type of network is used when the number of computers is relatively small and there is no need for centralized storage of files and network applications. Support for this type of network is built into all versions of operating systems and Microsoft: 95,98, Me, 2000, XP, Vista , 7, 8, 8.1, 10 including Home edition [5, 8, 15, 69, 128, 159]. Other advantages of this type of network include the low cost of construction, easy administration of each individual computer (node), the lack of need for a network system administrator who should take care of configuration and administration.

Client-server network

In this type of network the purpose of the individual machines is fixed from the very beginning there may be one (or several) server (s) controlling the access to resources and services of the connected workstations . Files can be stored centrally on the server and applications available for use by any computer, which means that if the server is turned on, each of the client computers can access the files at any time. In peer-to-peer networks [126-158], provided that the files are shared on one of the computers, there is a requirement that it not be stopped in order to provide access to certain information . The level of security in a machine from this type can be relatively easily enhanced thanks to centralized management, usually performed by the network administrator, who can also take care of centralized data archiving, application installation, user administration, etc. [12, 158, 225 , 321]. Networks of this type, in addition to being faster than peer-to-peer networks, allow the inclusion of more devices (not only computers, but also network printers, etc.), access to which is faster than peer -to- peer networks. On the other hand, the equipment for building this type of networks is many times more expensive, for their construction and administration a network administrator is needed, who, among other things, must deal with security issues, especially if the network is connected to the Internet. or to another network.

Combined type of networks

As you may have guessed, this type of network is a combination of the above two types of peer-to-peer network and client-server network. Very often due to the specifics of the tasks performed within an organization, this type of network is preferable [12, 56, 89, 90 -94]

Figure 1Combined network type

As can be seen from the diagram, a separate part of the network devices forming a workgroup forms a network with equal access, in which resources are shared between them without the involvement of the server [12, 54, 58, 95-112]. At the same time, the same computers are connected to a server that is part of a client-server network. Thus, on the one hand, the server controls the primary resources needed for the entire network, and on the other hand, does not allocate resources for managing devices needed only to work on computers in the workgroup connected to a peer-to-peer network [1].

OSI model

This model, OSI (Open System Interconnect), developed by the international standardization organization ISO, describes the structure of an ideal network connection [45, 58, 69, 226], using the concept of levels of

[1]https://www.it.souprovadia.info/node/29

interaction of network components. The OSI model contains seven levels of interaction that are relatively autonomous and can be distinguished [2].

Figure 2Levels of impact

LEVEL	MEANING	
1	Physically	
2	Channel	Media access control
		local link control
3 1	Network	
4	Transport	
5	Session	
6	Representative	
7	Applied	

of network components

1. Physical level - responsible for receiving and transmitting binary data. This level determines the electrical, mechanical and procedural characteristics of the channel between the end systems. It is the specifications [128, 128, 229] at the physical level that determine the voltage levels, the rate of transmission of physical information, fix the requirements for the environment for the transmission of information, etc.

2. Channel level - ensures the transportation of data below the physical level, ensuring the physical addressing the network topology, fault information, administration of information flow.

3. Network layer - is responsible for choosing the route between the two end devices, even if they are located in different geographical areas, as opposed to the physical layer, which monitors only the nearby network connections.

4. Transport level - the highest in the hierarchy of levels responsible for data transport. Provides monitoring of the integrity of sent or received data,

[2]http://pencho.my.contact.bg/start/comp/lan/lan.htm

controls the flow and sequence of data packets, provides mechanisms for the operation of virtual channels and troubleshooting systems [228, 229, 289, 291].

5. Session level - based on multiple network protocols establishes, manages and closes the sessions for interaction between applications, administering their requests.

6. Representative level - provides " readability " of the information sent from the representative level of one system to the same level of another system. For this purpose, this level can translate the sent information to some common format, understandable for the other system [128 -139].

7. Application level - ensures the implementation of user tasks, serving as an interface between the end system user and network services. At this level the co-operating applications are synchronized, the devices with which the connection will be established are identified, the amount of resources required for the presumed connection is estimated [128, 145, 156].

Wireless LAN (wireless communication devices)

Wireless networks

Until recently, when we mentioned this term, we immediately thought of mobile phones. But there are other areas where the convenience of wireless communications has pushed them to the back of the communication wave.

The use of radio channels to connect devices, although not new as an invention, has only recently evolved significantly, especially thanks to the widespread use of the Internet, local and WAN networks, connecting many people [3]to exchange voice, video and data with each other. and at noticeably high speeds [140-167].

The need for greater freedom and convenience in building networks, the need to easily connect the ever-increasing number of mobile subscribers who do

[3] https://www.bukvar.bg/materials/browse/11,148,,,,/?page=14&so=1

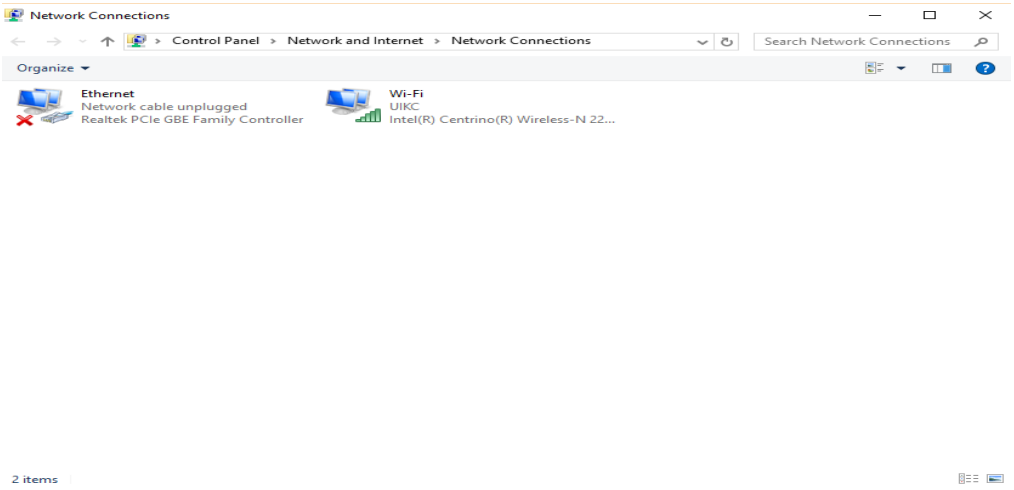
not want to look for special points to connect to the network, has given impetus to the development of wireless devices. globally - the need of modern man for modern high-speed and high-speed communications [5, 36, 56, 128, 259, 321].

Building wireless networks

Building wireless networks requires certain knowledge, not only in the selection of the necessary equipment, its deployment in the most appropriate way, but also in setting up software, access rights and technical security [45, 59 128, 149, 189].

The easiest way to connect two computers in a wireless network is to plug in each of them a WLAN card, no matter what interface it is (as long as it is supported), to install drivers, to set the necessary parameters connection, encryption levels, and the network is ready to exchange data between devices [5, 69, 128, 221].

The new generation operating systems such as Windows and Linux [221 - 240], after installing the necessary drivers , recognize the devices correctly and allow "communication" with them, as well as setting some parameters [4].



[4] http://pencho.my.contact.bg/start/comp/lan/wlan.htm

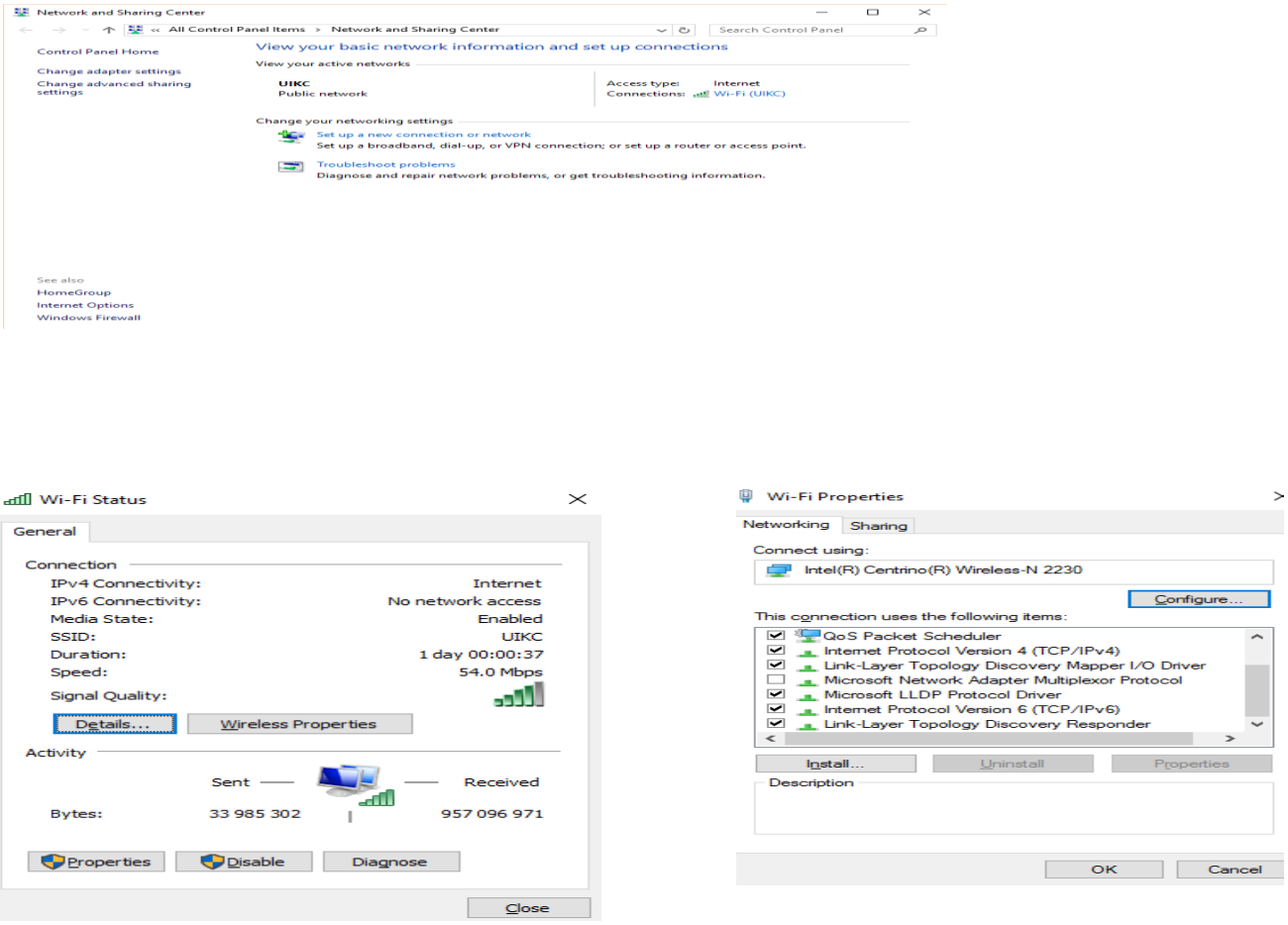


Figure 3Wireless network setup

Wireless communication devices (WiFi)

WiFi (Wireless Fidelity) is a type of WLAN - a wireless network designed for short-range use (up to 100 m indoors and up to 300 m outdoors), such as offices.

In order for a wireless network to be defined as WiFi , it needs to be built according to the requirements of the Wireless Ethernet Compatibility Alliance

(WECA). Compliance with these requirements ensures the compatibility of wireless devices, regardless of their manufacturer [25, 58, 258].

Advantages of using WiFi wireless devices :

- WiFi creates a "flexible" workstation where you can work anywhere and connect new users without adding additional connectors.
- WiFi allows you to connect to the Internet wherever there is a ' hotspot '.
- The standard allows office workers to use laptops, through which they can use the company's network from different locations, which makes them more mobile and flexible .

How the wireless network works [55, 98, 128, 157]:

In general, every WiFi wireless network has a HotSpot (literally a hotspot), through which all connections are made to the local network. It also provides the connection between the wireless network and other local area networks, as well as the connection to the Internet [159, 168, 191, 228, 289, 297].

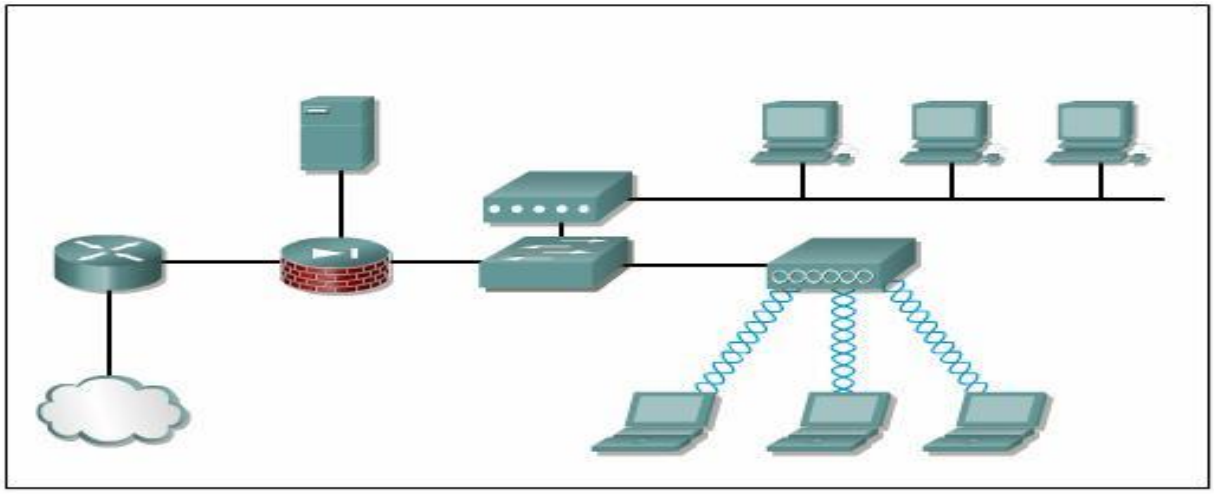


Figure 4Wireless data transmission system

Wi-Fi Direct

Wi-FiDirect , originally known as Wi-FiPeer-to-Peer , will soon become one of the main ways to wirelessly transfer data between devices.

Wi-FiDirect is a new standard for wireless data transmission that allows devices to connect directly without an additional router-like intermediate [225, 297, 310].

It is currently not possible to connect a printer directly to a computer or a phone to a laptop, so another router connector is required.

Wi-FiDirect is designed to remove this limitation and allow a direct connection between devices.

And whether Wi-FiDirect will be able to completely replace Bluetooth is difficult to say for sure now, but all the prerequisites are there. Compared to Bluetooth , the new Wi-Fi derivative is much better in terms of transmission speed and coverage, as well as data protection and ease of connection.

Getting rid of the redundant wireless interface in mobile devices will benefit both manufacturers and consumers because the devices become more compact, lighter, cheaper and simpler to manufacture. And users, instead of monitoring two interfaces, will do so to switch to only one [45, 56, 128, 159].

The new technology can be built into virtually any device, including those that traditionally work with Bluetooth (wireless keyboards, mice, headphones). To increase the autonomy of Wi-FiDirect , new energy-saving operating modes have been developed [158, 198, 197].

Specifications

Chapter Two OVERVIEW

The standard IEEE 802.15.4 / - ZigBee technology

ZigBee

ZigBee is a new wireless technology based on radio data transmission. This is an extremely flexible standard covering much of the needs of the wireless market. The technology also fills a big gap in the products offered so far. This is the first technology to offer very low power consumption, which is crucial for wireless devices [25, 39, 78, 118, 189].

IEEE 802.15.4 standard and Zigbee technology.

IEEE 802.15.4 is a standard implemented in May 2003. It is based on a simple protocol stack, with the aim of providing the hardware base for the further implementation of wireless applications covering the standard.

The ZigBee alliance, on the other hand, is an organization founded by several large corporations in the field of high technology (Philips, Motorola, Samsung, etc.), aiming to make existing technology usable and rent it on the market [185, 189, 199 , 228].

The organization creates wireless technology based on the IEEE 802.15.4 standard, adding to its capabilities and logical network topologies, as well as ensuring network security. It is important to note that the ZigBee alliance does not impose its own standard, but rather offers a ready -made set of solutions designed primarily for sensors and control systems [127, 158, 189].

Main features of the ZigBee standard

ZigBee technology has two data channels: 2.4 Ghz and 868/915 Mhz . At 2.4 Ghz channel frequency, data transmission takes place at a maximum speed of 250 kbps . In the case of lower frequency channels, the speed is lower - from 20 kbps to 40 kbps [125, 158, 225].

One of the main advantages of ZigBee is the low energy consumption. A device designed on the basis of this technology can run on a simple battery from a few months to 2 years, and in some cases even more. The distance at which a connection can be made is about 50 m (typical value) (from 5 m to 500 m

depending on the signal propagation environment). Data transfer is performed on the basis of negotiation (Hand-Shake protocols).

Another great advantage of ZigBee is the ability for devices designed on its basis to perform many different topologies - star (star), peer-to-peer , mesh and others.

Types of hacker attacks

WSN can be divided according to some functions. Some models are extremely simple: the sensor measures and sends data. Complex models involve the implementation of complex algorithms for operation and data processing. In the WSN security discussion, we need to explore what to protect ourselves from and what not. There are many forms and types of attacks [205, 289, 301]. We can divide them into: Passive attacks - eavesdropping, surveillance data collection, etc., Active attacks include fake appearance (Masquerade), replacement, modification, denial of services of service), etc. Of all, denial-of-service attacks are the most dangerous, as others can be protected by authentication and cryptography. Denial of service poses a threat to the entire system, which can be carried out with an unintentional random attack, but is likely to be targeted because in this case it is difficult to determine which of the participants is and where in the network. Attacks on WSN can be divided into several groups that follow:

Simple assembly (Simple Collection and Tranmittal):

- denial of services - denial of service
- transmission of fictitious data - broadcasting spurious information
- physical attacks - physical attack

• attack with forwarding of messages - replay attacks

The sensor node performs periodic measurements and sends them to the base station on the assumption that it is accessible and within range. These types of WSN is unstable to network-level attacks [201, 257, 258]. The denial-of-service attack consists of jamming or radio frequency interference, which initiates a collision. They are also susceptible to spoofing attacks in which malicious people attack by sending fictitious data . spurious information), resistant to physical attacks attack), such as theft, destruction, etc. Replay attacks on a previously sent message attack) are present here [16. 189, 190, 205].

Forwarding : _

• Black Hole

• Selective referral Forwarding

• Data Corruption _ _

• depletion of resources - Resource Exhaustion

The sensor collects them and sends the data to one of the neighboring sensors located on the way to the base station. Thus, the intermediate sensors forward the messages to the base station or to a neighboring sensor so that the data eventually reaches the base sensor. When receiving data, the sensor (in the first case) does not process it, it only transmits it on [15, 85, 94, 172]. Therefore, WSN is vulnerable to Black Hole attacks , data corruption, and resource depletion . Exhaustion). In the Black Hole attack, the node that is responsible for forwarding the data it repels (destroys). The attack on data corruption changes the content of the data during transmission [187, 186, 275]. The purpose of these attacks is to take control of the network. Depletion of resources takes place in such a way that the malicious person sends a large amount of data which is an unnecessary waste of energy resources (battery) [185, 189, 205]. When a packet has an explicit path that needs to be traversed, this is called selective forwarding

. Forwarding). Receiving and processing commands (Receive and Process Commands) [211, 267, 287]:

• sending fictitious (false) commands The sensor node receives commands from the base station that controls directly or through their neighbor (indirectly) another node, sending commands to change the state or actions. The ability to process commands is very useful for reducing the amount of data in the WSN. Commands can be sent to all nodes (broadcast) or to one (unicast). When sending to one node, it is necessary to provide some addressing of the nodes. Here comes the attack in which the malicious node takes on the property of a master node (base station) and sends fictitious (fake) commands. Self -Organization [15, 186, 211, 257] :

// atacks aginst routing protocol :

• spoofed , altered , or replayed routing information
• sinkhole attacks
• Sybil attacks
• wormholes
• HELLO flood attacks
• acknowledgment spoofing

WSN implementation is represented as just an organizational unit that learns and manages the topology. Network topology information can only be known on the base station or shared with some other second tier master nodes again with all nodes in the network [14, 52, 185, 199]. The nodes are then required to act as clusters so that they can solve the problem of network collision. WSN, in short, is sensitive to all attacks related to routing protocols (routing protocols) [158, 186, 194], here we will mention the Induced attacks Routing Loops , Sinkholes , Wormholes , HELLO Flooding . When the data in the structure of the

network itself can be tracked, the malicious person can change the data, resend it or invent it (spoofed , altered , or replayed routing information) [158, 856, 197]. This threatens the true figure of the network as seen by the base station.

Chapter three

GOALS AND TASKS

The aim of this dissertation is to study and analyze the transmission of data in different computer networks. Data transmission and reception (or, more broadly, data transmission or digital communication) is the transmission and reception of data (digital bitstream or digitized analogue signal over point-to-point or point-to-point communication).

Analog or analog transmission is a method of transmitting voice, data, image, signal or video information using a continuous signal that varies in amplitude, phase or some other property in proportion to the parameters of the variable. The messages are represented either by a sequence of pulses using a linear code (transmission in the main frequency band) or by a limited set of continuously changing signals (transmission in the frequency band) using the digital modulation method. Bandwidth modulation and corresponding demodulation (also known as detection) is performed by the modem hardware. According to the most common definition of a digital signal, both baseband and bandwidth signals representing bit streams are considered digital transmission, while an alternative definition considers only baseband signal as both digital and digital transmission. bandwidth data as a form of digital to digital conversion. - Analog conversion.

The data that can be transmitted can be digital messages from a data source, such as a computer or keyboard. It can also be an analog signal, such as a telephone call or a video signal digitized in bitstream , for example by means of pulse code modulation (CMS) or a more advanced output coding (analog-to-

digital conversion and data compression) circuit. This original encoding and decoding is done using the codec hardware.

From the analysis we can formulate the following goals in the present dissertation:

1. To make a systematic analysis of the different types of computer networks and to analyze the security of data transmission in them.
2. To develop mathematical models for information system analysis and to apply them to different computer networks.
3. Consider the various hacker attacks and ways to counter them.

The following tasks can be formulated from the goals made

1. Conceptual analysis of methods and approaches for analysis of computer networks and software systems

2. Overview of the different types of protocols and description of their differences - an overview of the topic.

3. Develop various software simulations using different protocols and analyze data transfer and some characteristics of the computer network such as data stability, bandwidth and more.

4. Application of new mathematical approaches to analyze and predict the stability of computer networks and information systems in particular.

5. Testing of computer simulations and realization of a hacker attack by analyzing different ways of entropy and the complexity of the attack

Discussion

Current next-generation network design research highlights the challenges that need to be overcome before applications and services that require high capacity, low latency and improved reliability can become the norm. Transport networks have a vital role to play in providing new and innovative applications and services that take full advantage of next-generation network architectures. The new software-defined network (SDN) [25, 33, 35, 44-50] has been successfully used to improve network solutions, such as data center and corporate networks, and current research is focused on the wider application of SDN-based network to the operator core and access networks, including wireless mobile feedback.

The software-defined network (SDN) paradigm has emerged.

over the last decade and is now ready to be fully adapted to transport networks. New technologies are constantly being developed that improve the productivity, reliability and resilience introduced to meet the rapid growth in data usage and the requirement for low latency and improved reliability.

The next generation of cellular networks, including 5th generation (5G) mobile cellular communications, will introduce improved quality of data transmission. Experience (QoE) and service quality (QoS) results that aim to meet the expectations of users and service providers. The next generation of cellular networks are seen as favorable factors for the network society, where they are ubiquitous [43, 66, 161]. High-speed data connections will be available to connect users and devices to the network. The growth of machine-to-machine communications and the expected addition of hundreds, millions of devices led to the emergence of the term Internet of Things (IoT). Adopted to highlight the

growth and change that must occur by introducing next-generation cellular networks.

Research and development of new technologies and systems for the Radio Access Network (RAN) has introduced transport network related challenges that need to be overcome to ensure that the next generation cellular networks work as expected and facilitate growth [25, 132, 164] in new and innovative applications and services. With earlier generation cellular networks, it may have been possible, in some circumstances, to over-provide the transport network, thus eliminating the need for complex transport network design and the use of technologies that improve the operation of transport networks. Excessive security of the transport network ensures that this does not become an obstacle between the core and RAN, however, the total cost of ownership for transport networks has increased as cellular networks have expanded, leading to the adoption of cost-cutting strategies. The introduction of small cells, pico cells, and ultra-dense small cell networks (UDNs) [86, 100, 112] have created architectural, challenges to provide and optimize for future transport network projects [111-118].

Tested on a computer system with Raspberry PI by the brute force method

Description of the algorithm

1. Introduction

The purpose of this text is to illustrate how a Raspberry mini computer works Pie 3 can be used for WIFI hacking. (you can add brief technical specifications for the device).

2. Need Hardware / Need Components

- Raspberry Pie 3

- Micro SD card (16 GB)

- Card reader (USB Micro SD Card Reader) - used to copy the updated firmware from our computer.

- Ethernet cable - Used to connect Raspberry Pie 3 and WIFI router. It is needed to be able to control Raspberry Pie 3 from another device that is also connected to the router.

- Adapter (2.5 Amps) - power supply

3. Install the Firmware

In principle , the inspection mode (monitor mode) of Raspberry Pie 3 does not work. In order to use it, we must first install the updated firmware .

We can update the firmware as follows:

- We download the firmware to our computer

- We put / Turn on Micro SD card in the slot

- Extract (E xtract) the downloaded file with Winrar (Windows) or Unarchiver (Mac)

3.1 Installation in Windows

We need to install Win 32 Disc first Imager . Then open the program, highlight the extracted / unzipped file and press write .

It's not bad to have a screen shot here or more precisely cut only the program window with snipping tool as in the video

3.2 Installation in IAC

First we open a terminal where we write **discutil list .** With this command we identify which disk is our SD card. Then we use the **diskutill command unmountDisks Disk 1 (** as Disk 1 in this case is our SD card **)** .

We continue with **Sudo dd bs = 1 m if [** the path to the image] of = / dev / rdisk 1 (as Disk 1 in this case is our SD card). Then we wait for the command to execute.

The next step is to plug the SD card into the Raspberry Pie 3. Then connect the device to the router via Ethernet cable. The last step to turn everything on and off is to turn on the power adapter.

4. How to find the IP address of Raspberry Pie 3

So we can run Raspberry Pie 3, we need to know the local IP address of the device . There are many different methods to find his address. The proposed methods use software to scan IP addresses, in this case we use Angry IP Scanner .

Once we find the Raspberry IP address Pie 3, we can now control it.

5. Control Raspberry Pie 3 (Windows and Mac)

Windows

First we need to download additional software, in this case Putty.

After loading the application, enter the IP address of Raspberry Pie 3.

Sign in as **Root (Login as: Root)**

We enter the password, which by default is **toor .**

MAC

Open a terminal and enter the following: **ssh root @ 192.168.1.113 [address is example -** Raspberry IP address must be entered Pie 3].

Everything is now configured and working and we can start hacking.

* We can also use terminal emulator to establish ssh connection through our Android smartphone.

6. WIFI Hacking

We need to follow certain steps as follows to complete the WIFI hack successfully.

1. Find the file that contains the password for the WIFI network (*. Cap)

2. Copy the Raspberry password list Pie 3 through Ù SB .

3. Execution of wordlist attack against. file cap

6.1 Finding / capturing the file that contains the password for the WIFI network (*. Cap)

We open the connection to the Raspberry terminal Pie 3. Write the **monstart command** to run the network card check mode, then enter **airodump - ng wlan 0** to see all routers in range.

For the purpose of this text, we will assume that the network of the router we are hacking is called **Wireless Network** . Once we identify the network we are looking for, we need to capture the handshake file that contains the password for the router 's WIFI network.

To perform this task, we need to write down the channel number (№6 in our case, as well as the BSSID .

Press ctrl + C to stop the process and return to the command field (command line). Then we enter the following:

Computer simulations of various protocols with the Matlab software package

A network can be _ organized in two ways:

as equal (peer to peer) a workgroup in which each computer can act as a client or server, with each user administering their own computer resources;

as a server-based network, the administration of which is concentrated in a central computer called a server.

Equal networks are suitable for small networks involving no more than 10 computers . All computers in one such a network form a common working group (workgroup). This requires each of the computers to be configured to work in a workstation group . In Windows this is done by setting up the computer for networking, such as the name of the worker group should be _ the same for each of the computers .

In server-based networks, access to resources is controlled through *authentication* (*authentication*) and *permissions* (*permissions*). For everyone shared resource the network administrator assigns permissions (access rights) for each individual user or for an entire working group . Permissions are indicated _ resource access levels , such as whether a file is read- only or can be in it changes made (edit or delete) [7-10].

In this new information age, high data speeds and high reliability are pushing our wireless systems forward and becoming a dominant factor in the successful deployment of commercial networks. MIMO-OFDM (Multiple Input Multiplexing and Orthogonal Frequency Split), a new wireless broadband technology, has gained great popularity due to its high-speed transmission capabilities and reliability against multi-channel attenuation and other channel interference. The main challenge for MIMO-OFDM systems is how to accurately and quickly obtain channel status information for sequential information symbol detection and channel synchronization. In the first part of the paper a problem for channel estimation for MIMO-OFDM systems is formulated and an estimation algorithm based on pilot tone is proposed.

A complex equivalent model of MIMO-OFDM signals with a baseband is represented by a matrix representation. By selecting equally spaced and equally powerful pilot tones from the subcarriers in one OFDM symbol, a reduced discrete version of the original signal model is obtained. In addition, this signal model is converted to a linear form, which is solvable for the LS (least squares) estimation

algorithm. Based on the obtained model, a simple design of pilot tones in the form of a single matrix is proposed, the rows of which represent different sets of pilot tones in the frequency domain, and the columns of which represent different transmitting antennas in the spatial domain. From the analysis and synthesis of the pilot tone design in this development, our estimation algorithm can reduce the computational complexity inherited in MIMO systems from the fact that the pilot tone matrix is essentially a single matrix and has been proven to be the optimal channel estimator. in the sense of achieving a minimum.

MSE (root mean square error) estimates of the channel for fixed power of the pilot tone. The second part of this dissertation deals with the problem of wireless location in WiMax (global microwave compatibility) networks, which is based mainly on MIMO-OFDM technology. From the TDOA (Arrival Time Difference), AOA (Arrival Angle) or a combination of the two, a quasi-linear LS solution form is formulated. It is assumed that the observation data are distorted by zero average AWGN (additive white Gaussian noise) with very small variance. According to this assumption, it is proved that the term quasi-linear noise has an approximately normal distribution. Therefore, the ML (maximum probability) estimate and the LS solution are equivalent. But the ML estimation technique is not applicable here due to its computational complexity and the possible lack of an optimal solution.

IMO-OFDM systems are the norm in modern wireless systems (eg 5G NR, LTE, WLAN) due to their reliability for frequency selective channels and high data rates. With the ever-increasing requirements for maintained data rates, these systems are becoming more complex and large in configurations with an increasing number of antenna elements and special resources (subcarriers).

With antenna arrays and spatial multiplexing , efficient transmission techniques are needed [6]. Beamforming is one such technique used to improve

the signal-to-noise ratio (SNR), which ultimately improves the system performance measured here in terms of bit error rate (BER) [1].

This example illustrates an asymmetric single-user MIMO-OFDM system, where the maximum number of antenna elements at the transmitting and receiving ends can be 1024 and 32, respectively, with 16 independent data streams. It simulates a spatial channel where array locations and antenna models are incorporated into the overall system design. For simplicity, single point-to-point communication (one base station interacting with one mobile user) is modeled. The channel uses the sound of the channel to provide the transmitter with the channel information needed to form a beam.

The example offers a choice of several spatially defined channel models, in particular the WINNER II channel model and the scatter-based model, both taking into account the spatial transmission / reception locations and the antenna models (Figs. 27 and 28).

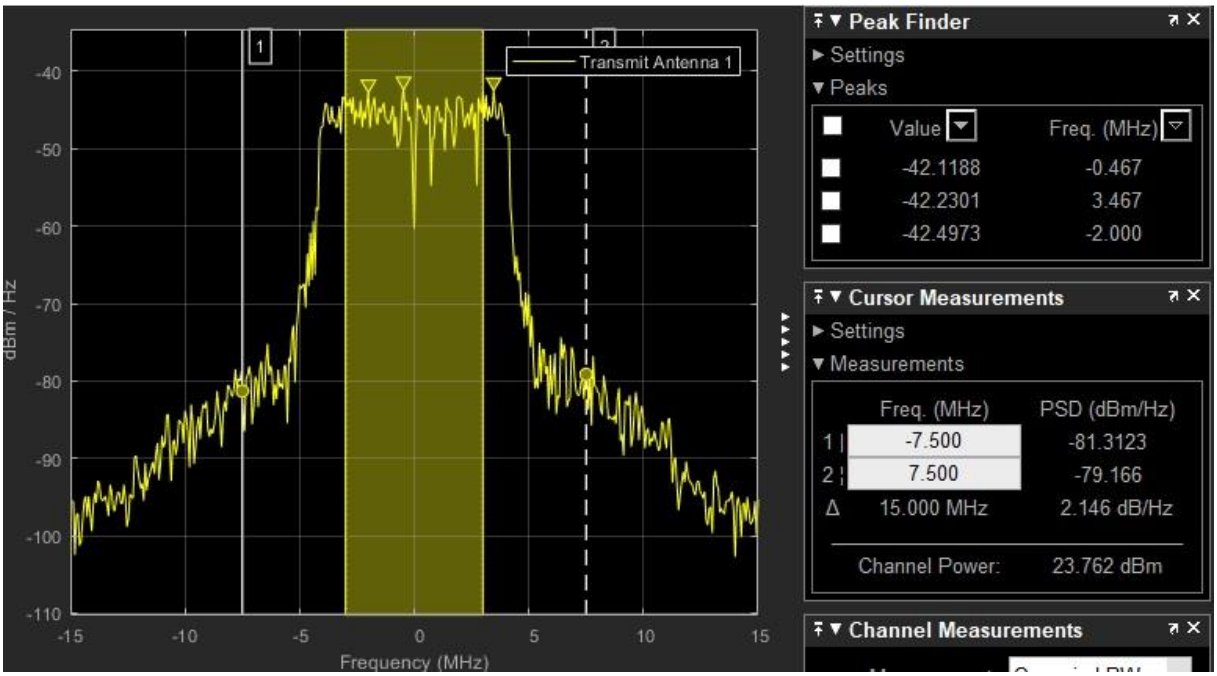


Figure 5Bandwidth analysis of a computer network with matlab

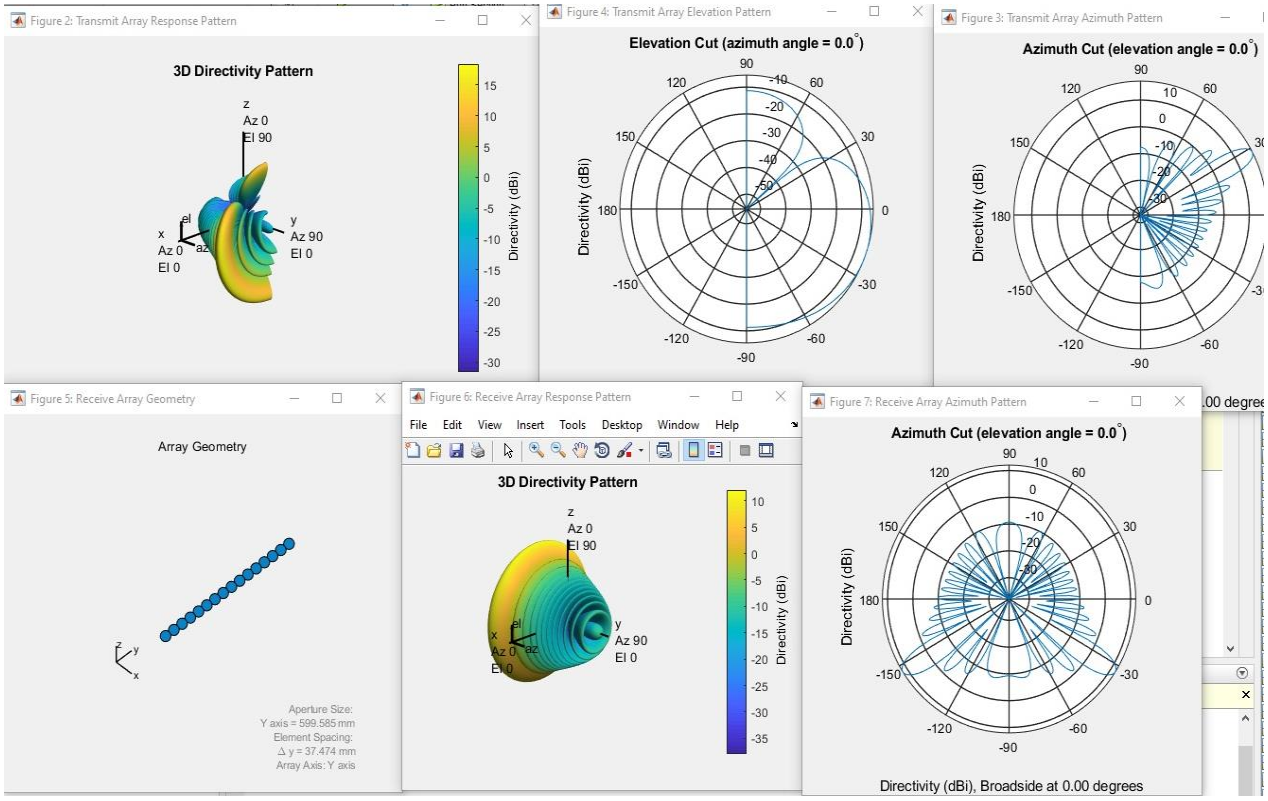


Figure 6Simulation of data transmission and noise analysis with matlab 2018 work with MIMO - OFDM package Precoding with Phased Arrays[5]

5 Perahia, Eldad, and Robert Stacey. Next Generation Wireless LANS: % 802.11n and 802.11ac. Cambridge University Press, 2013 .

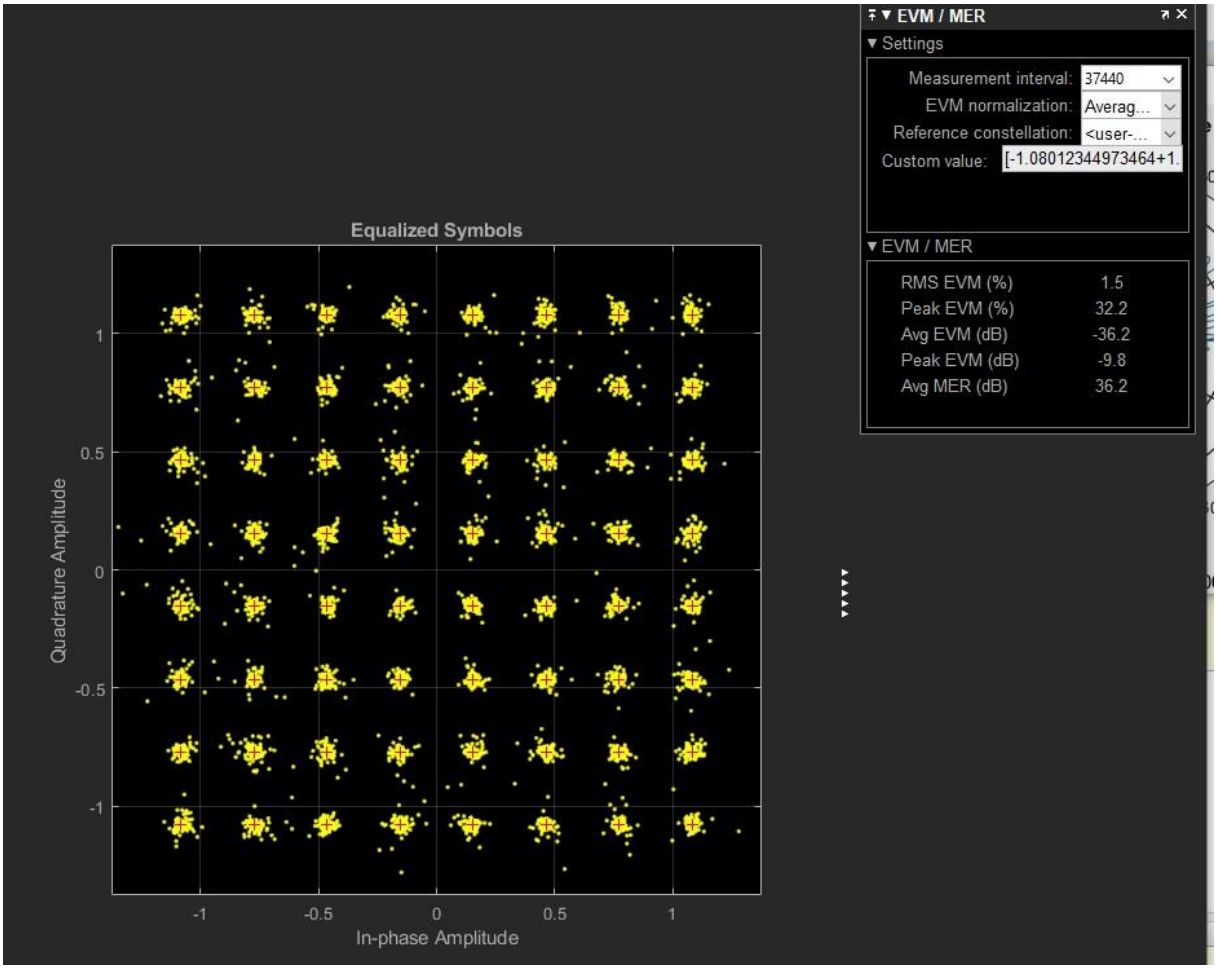


Figure 7Noise dissipation - matlab 2018 work with MIMO-OFDM Precoding package with Phased Arrays

MATHEMATICAL MODELS FOR COMPUTER SYSTEM ANALYSIS

Game theory

In game theory, opponents are called players. Each of them has many possible moves. It can be finite or infinite. Possible actions are called strategy games. Outcomes or payments are defined by features that depend on the player's strategy.

A two-player matrix game is a zero-sum game in which the sum of the winnings of the first and second players ν_1 and ν_2 is zero:

$\nu_1 + \nu_2 = 0.$

If the first and second players choose a mixed strategy x = ($x_1, x_2, \ldots x_m$) for y = ($y_1, y_2, \ldots y_m$), then the mathematical expectation of the first player's profit is

$$E(x,y) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} x_i y_j$$

Let X and Y be the sets of mixed strategies of x and y.

The question arises about the existence of an optimal strategy x^* and y^* for profit (loss) of the first, respectively the second, ie. the mathematical expectation for the first is the maximum gain (respectively loss) is the maximum in the best game of the opponent.

According to the basic theorem of game theory, there are optimal strategies x^* and y^*, ie. for a matrix game with zero sum there is a solution

$$\max_{x\in X}\min_{y\in y} E(x,y) \quad = \quad \min_{y\in y}\max_{x\in X} E(x,y) \quad = E(x^*,y^*) = \upsilon$$

So for every $x \in X$ and $y \in Y$ is satisfied

$$E(x^*,y) \le E(x^*,y^*) \le E(x,y^*)$$

The number $\upsilon = E(x^*,y^*)$ is called the price of the game, and the point at which it is reached is called the saddle point [6].

If we interpellate the presented results, if we have two players in one cyber system, one defends himself, the other attacks, there is always an optimal strategy for defense, respectively attack [7].

---

6 Vladimir Mazalov Mathematical Game Theory and Applications, Wiley, 2012, ISBN 978-1-118-89962-5

7 Vito (2021). Game Theory (https://www.mathworks.com/matlabcentral/fileexchange/51601-game-theory), MATLAB Central File Exchange. Retrieved November 10, 2021

$t = 0$

Let's look at another strategy L players (hackers) attack, N / L are the attacking computers - the second players.

Using the model of Hamilton - Jacobi - Bellman

$$\widehat{V}_L(x) = \max_{u_i \in L} \lim \left\{ \sum_{i \in L} \log u_i + \varepsilon \widehat{V}_L \left(\varepsilon x - \sum_{i \in L} u_i - \sum_{i \in N \setminus L} \widehat{u}_i \right)^{\alpha} \right\}$$

$$\widehat{V}_L(x) = \max_{\widehat{u}_i \in N \setminus L} \lim \left\{ \sum_{i \in L} \log \widehat{u}_i + \varepsilon \widehat{V}_L \left(\varepsilon x - \sum_{i \in L} u_i - \sum_{i \in N \setminus L} \widehat{u}_i \right)^{\alpha} \right\}$$

Search for a solution in the following form

$$\widehat{V}_L(x) = \widehat{A}_L \log x + \widehat{B}_L \text{ , } \widehat{V}_i(x) = \widehat{A}_i \log x + \widehat{B}_i$$

as follows $u_i = y_i^K x, i \in L$,. $\widehat{u}_i = \widehat{y}_i^K x$

For an optimal solution we get the following coefficients

$$V_i^k = \frac{1-a}{k(1+(n-k)(1-a))} \delta x$$

$$\widehat{V}_L(x) = \frac{k}{1-a} \log x - \frac{1}{1-\delta} \widehat{B}_L \text{ .}$$

$$B_L = k \left(\frac{1}{1-a} \log \left(\frac{\delta}{1+(n-k)(1-a)} \right) + \log(1-a) + \frac{a}{1-a} \log(a) - \log(k) \right)$$

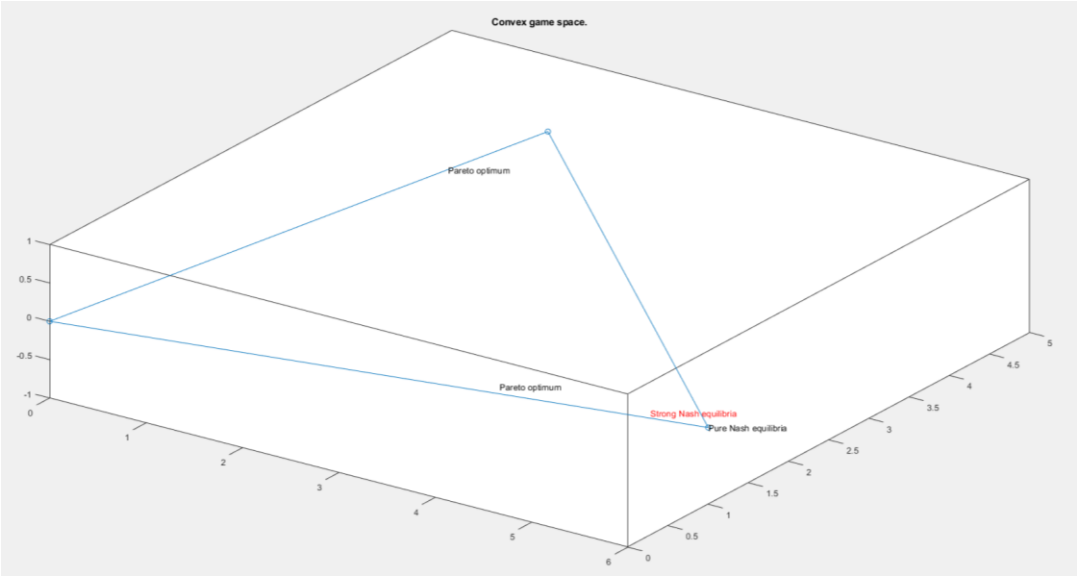


Figure 8Solution of a matrix game in the Pareto sense

Yields

Based on the research and analysis, the dissertation offers the following scientific and applied contributions:

1. Problem areas in the field of information exchange in different computer networks have been identified and a systematic review has been made.

2. The various methods of hacker attacks are presented and methods of their protection. This group of attacks includes any attempt to gain unauthorized access to the system. An analysis of the different types of attacks has been made, such as :

    - Denial of Service (DoS) attacks: A type of attack that causes a loss of service or inability of the network to function.
    - • Web attacks: this is any attack that tries to disrupt / alter a website. Two of the most common such attacks are: SQL injection (SQLi).
    - • "Hijacking" of HTTP sessions (Session hijacking): these attacks are a hijacking of the user session ID hijacking).
    - • DNS poisoning : This type of attack compromises the DNS server so that users can be redirected to malicious websites.

3. A method of hacker attack using the brute force method has been developed. Implemented d with a hybrid computer of the Arduino type . An analysis of the complexity of the attack was made.

4. Mathematical models for the analysis of the stability of the security of a computer network and ways for the annals of this system have been developed. Mathematical approaches such as Markov processes, Theory of games with nature using the Bellman principle and Theory of catastrophes were used.

5. Matlab software package , numerous simulations have been made to analyze the data transfer in different computer networks and the influence of noise on this transfer.

6. The traffic on the computer network of the Internet provider is analyzed and the main attacks on the provider are systematized.

7. A conceptual analysis of the types of computer attacks and their ways of conducting on budget enterprises has been made .

Conclusion

The topic of networks, even wireless networks, is really huge and cannot be covered in just one development. I hope that with this material I have given you some initial information and guided you in terms of what exactly is the most common wireless technology at the moment and their access protocols.

Comparing the two types of communications - wired and wireless, one can see significantly more advantages over wireless than disadvantages, even compared to Ethernet . Undoubtedly, technology will continue to evolve at an ever-increasing pace, clearing up errors and inaccuracies, increasing exchange rates and taking better care of storing our valuable data.

The protocols for access to the communication environment in wireless local area networks differ from the protocols for multiple access in cable networks due to the changing parameters of the communication channel and the phenomenon of hidden terminal.

The use of a common MAC protocol for ISM radio channels and diffuse infrared channels complicates the protocol. The current 802.11 MAC protocol shows good results mainly for radio channels.

A modification of the protocol for access control to the communication environment in wireless local area networks with diffuse infrared channel is proposed, which solves the problem of possible conflicts in the exchange of data frames and the presence of hidden H2 type stations on the network .

LIST OF PUBLICATIONS

by Ilian Vladimirov Ivanov

Full-time PhD student in the Department of Communication and Computer Engineering and Technologies

at the Technical Faculty

of SWU "Neofit Rilski", Blagoevgrad

Articles

1. Trenchev , I., Stoykov , D., Traykov , M., Stefanov , A., Trencheva , M. **, Ivanov , I.** , (2020) ***Create 3D models by explicitly describing and moving the virtual camera using EEG Signals*** , in proceeding The Future of Education - 10th edition , 18-19 June 2020, ***(Indexed in Web of Science)***

- https://conference.pixel-online.net/FOE/files/foe/ed0010/FP/6778-ICT4765-FP-FOE10.pdf

2. Stefanov , A., **Ivanov , I.** , Trenchev , I., Stoev , R., Trencheva , M. **,** (2020), ***Usage of mathematical models for cybersecurity analysis*** in proceeding The Future of Education - 10th edition , 18-19 June 2020 , ***(Indexed in Web of Science)***

- https://conference.pixel-online.net/FOE/files/foe/ed0010/FP/6778-HED4764-FP-FOE10.pdf

Reports in scientific forums (conferences)

1. Ivanov, I., (2021), " ***Research of local networks with software*** ", Ninth National Seminar on" Intellectual Property in the New (Un) Normal ", pp. 183 - 189, Sofia, April 26, 2021 / in press /.

2. Ivanov, I., (2021), " ***Training in multimedia and cloud technologies*** ", Ninth National Seminar on" Intellectual Property in the New (Un) Normal ", pp. 177 - 182, Sofia, April 26, 2021 / in press /.