РЕЗЮМЕТА НА НАУЧНИТЕ ТРУДОВЕ И УЧЕБНИ ПОСОБИЯ

на доц. д-р инж. Венета Панайотова Алексиева
за участие в конкурс за заемане на академичната длъжност: ПРОФЕСОР
по професионално направление
5.3 „Комуникационна и компютърна техника”
Учебна дисциплина „Компютърни мрежи“,
към катедра „Компютърни науки и технологии“
Факултет по изчислителна техника и автоматизация
обявен от Технически университет – Варна,
ДВ, извънреден брой 110 от 24.12.2021 г.

Резюметата на научните трудове са организирани в раздели както следва:

	Трудове за участие в конкурса за „Професор“	**брой**
В.4	**Публикации равностойни на монографичен труд на тема „Методи и средства за повишаване на Quality of Services (QoS) в безжични мрежи”**	**16**
Г	**Публикации извън групата на монографичния труд**	**37**
Г.7.	Публикации в реферирани и индексирани в световноизвестни бази данни с научна информация	13
Г.8.	Публикации в нереферирани списания с научно рецензиране	24

В.4 Публикации равностойни на монографичен труд на тема „Методи и средства за повишаване на Quality of Services (QoS) в безжични мрежи”

В.4.1. Veneta Aleksieva, Hristo Valchanov and Diyan Dinev, Comparison Study of Prototypes based on LiFi Technology, 8-9.11.2019, Varna, BIA2019, p.73-76, ISBN 978-1-7281-4754-3, IEEE Catalog number: CFP19U85-ART, DOI: 10.1109/BIA48344.2019.8967478

В този доклад е предложен LiFi прототип за комуникация на данни и сравнително проучване на предложения от авторите LiFi прототип с други подобни LiFi прототипи (P.Goswamis и LiFiNano). Ограниченията на предложения прототип са:

• Максималното разстояние на предаване е когато LED крушката излъчва под ъгъл 90^o с хоризонтална равнина. Този ъгъл гарантира максималното разстояние на предаване от 80 см. Този резултат се постига в напълно тъмна стая.

• Колкото повече се намалява ъгъла на излъчване на LED крушката, толкова повече намалява разстоянието за успешно предаване. Когато ъгълът е по -малък от 40^o, получаването на данни е неуспешно.

Изследването на предложения прототип се фокусира върху въздействието на някои фактори на околната среда (като осветеност на слънчевата светлина, стъклена преграда и солена вода). Експериментите с прототипа са направени, за да се определят неговите ограничения за максимално разстояние на предаване при различни условия на околната среда.

Целта на настоящото изследване е да се съберат данни за предаване през различна среда. Използва се LiFi прототип, разработен в предишно изследване, но в софтуера са направени някои подобрения, като например подобряване на скоростта на предаване и корекция на грешки.

Директната слънчева светлина (в този експеримент - 7520 лукса) води до 100% загуба на предадената информация към приемника, дори ако е на 1 см от предавателя. Намалява се осветеността на слънчевата светлина, като се отдалечава прототипа от прозореца, тогава разстоянието Dmax се увеличава. При достигане на 2,5 м (200 лукса), Dmax е 60 см. Стойността на Dmax от 80 см се достига на разстояние 4,0 м от прозореца (където въздействието на слънчевата светлина е 0 лукса). Това е същото като Dmax, което се достига в напълно тъмна стая.

Ако дебелината на стъклена преграда е само 2 мм, разстоянието е същото като разстоянието без преграда. Но ако дебелината на стъклената преграда расте, Dmax намалява. При стъклена преграда от 12 см Dmax е само 40 см - половината от максималното разстояние.

Бяха проведени експерименти с прясна и солена вода (10% и 20% солен разтвор). Въздухът е изключен, тъй като модулите на предавателя и приемника са залепени за стъклото на аквариума. На разстояние 55 см само при 0% соленост има комуникация, но на разстояние 26 см има комуникация и при 20% солен разтвор.

Избрани са основни показатели за ефективност за оценка и сравнение на прототипа, предмет на гореспоменатите експерименти, и други прототипи на LiFi. Въз основа на тях се прави сравнението. Прави се комплексна оценка - средна аритметична и средна геометрична. По отношение на резултатите от комплексните оценки може да се заключи, че авторовият LiFi прототип е най - добрият вариант за целите на настоящото изследване.

B.4.2. Haka, V. Aleksieva and H. Valchanov, "Comparative Analysis of Traffic Prioritisation Algorithms by LTE Base Station Scheduler," 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), Bourgas, Bulgaria, 2020, pp. 1-4, doi: 10.1109/SIELA49118.2020.9167040.

Този доклад представя изследване на въздействието на предложения от авторите алгоритъм за приоритизиране на трафика в LTE мрежа, Round Robin (RR), Maximum Rate (MAX-Rate), Proportional Fair (PF), Exponential/Proportional Fair (EXP-PF) и тези, предложени от Myo и Akyıldız за QoS в 4G LTE безжична мобилна мрежа.

Сравнението се основава на резултатите от пропускателната способност, забавянето, коефициента на предаване на пакети (PDR) и коефициента на загуба на пакети (PLR). За да се проучи въздействието на алгоритмите за приоритизиране на трафика върху QoS, се използва продуктът за симулация на LTE, предложен и допълнително разработен от авторите.

Експериментални проучвания се провеждат за статични и мобилни UE за една LTE клетка, за която предавателната мощност е 40W (46.02dBm), 20 MHz честотна лента, мощността на шума е -160.99dBm, 100 налични PRB, 6 секторни клетки и радиус 770m. Брой потребители са съответно 20, 50, 70 и 100. Разстоянието на статичните UE до използвания eNodeB (m) е съответно 10, 90, 170, 250, 330, 410, 490, 570, 650 и 730 (55 м за всички мобилни UE). Изискваният вид услуга е GBR, задължителните RB от всяко UE са 5555 и плащат цена за гарантирана услуга със стойност 5. Скоростите на движение за мобилни UE (km/h) са съответно 10, 20, 30, 40, 50, 60, 70, 80, 90 и 100.

Представените резултати показват, че с по -малък брой абонати, предложеният алгоритъм осигурява по -високи стойности за изследваните параметри за статични абонати, разположени в обхват до 250 метра от eNodeB и осигурява по -високи стойности за изследваните параметри за мобилни абонати, движещи се с не повече от 80 км/ч. С увеличаването на броя на абонатите обслужването става равномерно, но за абонатите с най -висок приоритет се осигуряват по -добри стойности, докато за другите алгоритми резултатите са почти еднакви.

Предимството на предложения алгоритъм пред другите е, че той обслужва заявки с висок приоритет от абонати на по -близко разстояние до eNodeB и заявки от мобилни абонати. Обслужването на заявки от абонати, разположени по -близо до eNodeB е с по-добро QoS, тъй като качеството на канала на тези абонати е по -добро грешките при предаване са по -малко, което води до по -бързо обслужване. Приоритетната услуга за заявки от мобилни потребители подобрява QoS за тях, тъй като това намалява загубите на пакети при предаване. Разпределянето на повече ресурси към потребителите с по -висок приоритет ще ускори обслужването на техните изисвкания и освободените от тях ресурси ще се използват за обслужване на UE с нисък приоритет.

В.4.3. Haka, V. Aleksieva and H. Valchanov, "Comparative Analysis of Traffic Prioritisation Algorithms in 6LOWPAN Networks," 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), Bourgas, Bulgaria, 2020, pp. 1-4, doi: 10.1109/SIELA49118.2020.9167116.

Този доклад представя цялостен сравнителен анализ между предложения от авторите алгоритъм за приоритизиране на трафика на 6LoWPAN сензорна мрежа и пет стандартни алгоритма на сензорната мрежа. Има два основни класа алгоритми за приоритизиране на трафика за сензорни мрежи: Knowledge Free и Knowledge Based. В алгоритъма на авторите, според първоначалното приоритизиране, планирани заявки с най-висок приоритет съдържат Emergency Dispatch Header. Той идентифицира пакета като спешен. В случай на множество пакети със Emergent Dispatch Header или обикновени пакети, заявките от мобилни устройства се обслужват с по-висок приоритет. Когато са налични много подвижни устройства, техните заявки са приоритизират, като се използва скоростта им на движение. С по -висок приоритет се обслужват заявки от по -бързо движещи се устройства. При наличието на множество мобилни устройства, движещи се с еднаква скорост, следващият критерий, по който заявките се приоритизират, е разстоянието на сензора до координатора. За тази цел е използван принципът на Least Weighted Farthest Number Distance Product First mechanism. По-висок приоритет имат пакетите, изпратени от най-близките до координатора сензори. Когато на еднакво разстояние до координатора има много сензори, заявките се приоритизират, като се използва типа на сензора. С най-висок приоритет са приложенията за здравни грижи, след това са за сигурност и наблюдение, мониторинг на околната среда, проследяване на животни, проследяване на превозни средства, земеделие и интелигентни сгради.
Авторите са създали симулатор, който се използва за изследване влиянието на предложения алгоритъм и стандартни алгоритми за приоритизиране на трафика върху QoS в една и съща сензорна мрежа.
Представен е подробен сравнителен анализ на предложения от авторите алгоритъм за приоритизиране на трафика за 6LoWPAN и пет други. За комплексно сравнение на алгоритми за приоритизиране на трафика в 6LoWPAN е предложена система от критерии. Сравнение на алгоритмите за приоритизиране на трафика се прави по закъснение, пропускателна способност, Packet Delivery Ratio и Packet Loss Ratio. Това сравнение е направено за конкретен тип трафик, за определени крайни възли.
Предложеният от авторите алгоритъм за приоритизиране на трафика в 6LoWPAN е по-добър от другите изследвани, според средните аритметични и средните геометрични комплексни оценки.

B.4.4. Haka, V. Aleksieva and H. Valchanov, "Software Tool for Evaluation of Traffic Prioritisation Algorithms in 6LOWPAN Network," 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), Bourgas, Bulgaria, 2020, pp. 1-4, doi: 10.1109/SIELA49118.2020.9167147.

Този доклад представя подобрения в симулационния продукт за 6LoWPAN мрежи, предложен от авторите, който дава възможност за изследване на качеството на услугите. Разгледано е влиянието на различни алгоритми за приоритизиране на трафика върху пропускателната способност, забавянето, packet delivery ratio и packet loss ratio. Включените алгоритми в софтуерния инструмент са: предложения от авторите алгоритъм и класическите алгоритми за приоритизиране: First Come First Served (FCFS), Least Number of Sensors First (LNSF), Least Number of Hops First (LNHF), Least Number Distance Product First (LNDPF), Least Weighted Farthest Number Distance Product First (LWFNDPF). Софтуерният инструмент предоставя интерфейс за оценка на предложения и класическите алгоритми в сензорните мрежи.

В предложения симулатор броят на сензорните възли, работещи в даден регион, може да варира до 100, в зависимост от размера на зоната, която трябва да бъде покрита. Устройствата в тази област могат да бъдат напълно функционални или с намалена функционалност. Напълно функционалните устройства могат да работят както като координатори, така и като крайни възли, докато тези с намалена функционалност работят само като крайни устройства.

6LoWPAN сензорна мрежа е симулирана с едно напълно функционално устройство, което обслужва заявките на крайните устройства. Целта на изследването е да се определи ефективността на алгоритмите, вградени в симулатора за приоритизиране на трафика и в кои ситуации, за кои възли те подобряват QoS.

Резултатите от предложения алгоритъм за приоритизиране показват, че стойностите за изследваните параметри са по-добри за статичните устройства, които са по-близо до координатора. Приоритизирането на заявките от възли, които са по-близо до координатора в сензорните мрежи, е важно, тъй като те са мрежи от множество устройства, които предават данни постоянно. Това причинява смущения в комуникационната среда и грешки, което инициира повторното изпращане на пакети. В резултат на това натоварването и забавянето на комуникацията се увеличават и влошават QoS. С по-малко устройства, заявките с най -висок приоритет се обслужват с повече ресурси - от възлите, разположени до 6 метра от координатора. Това ускорява обслужването за тези възли, като същевременно освобождава ресурси за използване за устройства с нисък приоритет и компенсира закъсненията. В случай на недостатъчни ресурси, заявките на устройства с най-нисък приоритет се отлагат за обслужване в следващия интервал от време.

Резултатите за мобилните възли съгласно предложения алгоритъм за приоритизиране показват, че стойностите за изследваните параметри са по-добри за възлите, движещи се със скорости над 3 m/s.

B.4.5. D. Dinev, V. Aleksieva and H. Valchanov, "Study of Li-Fi Indoor Network Reliability", 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), Bourgas, Bulgaria, 2020, pp. 1-4, doi: 10.1109/SIELA49118.2020.9167053.

В този доклад е предложено внедряване на тестова Li-Fi мрежа на закрито. Реализираната мрежа се състои от три LiFi точки за достъп в стаята за предаване на информация на разстояние 2,5 м от пода. Всяко от устройствата LiFi е на разстояние 75 см от съседното устройство. Максимален ъгъл на осветяване, при който устройствата предават информация е 45^{o}.
Целта е да се реализира хендовер от потребителско оборудване (UE) между LiFi точки за достъп на физически изградената мрежа, като се вземат предвид правилно и неправилно получените данни по време на този процес. Реализацията на хендовер в Li-Fi мрежи е много важна за повишаване на надеждността на мрежата и предаване на всички данни преди напускане на мрежата.
Бяха проведени следните експерименти:
- да се определи работоспособността на мрежата;
- да се извърши хендовер на потребители от една точка за достъп до друга съседна;
- докладване на правилно и неправилно получени данни;
По време на експериментите светлината в стаята беше средно 16,6 lx.
За първата група експерименти бяха използвани следните параметри:
- брой изпратени знаци - 10 000;
- скорост на движение на потребителското оборудване - 1m/s, 2m/s и 3m/s
- разстояние между предавателя и приемника (L) - 0,5 м, 0,8 м, 1 м, 1,2 м и 1,5 м;
От резултатите, получени чрез експериментите, може да се види, че при нормална скорост от 1 m/s всички данни, изпратени от предавателя, са били успешно получени без загуби или погрешно получени пакети при преминаване от една точка на достъп до друга. Това е така за всяко от измерените разстояния между предавателя и приемника. С увеличаване на скоростта се наблюдава увеличаване на процента на неправилно получени или неполучени данни.
За втората група експерименти бяха използвани следните параметри:
- брой изпратени знаци - 100 000;
- скорост на движение на потребителското оборудване - 1m/s, 2m/s и 3m/s
- разстояние между предавателя и приемника (L) - 0,5 м, 0,8 м, 1 м, 1,2 м и 1,5 м;
От резултатите, получени чрез експериментите, може да се види, че при нормална скорост от 1 m/s почти всички данни, изпратени от предавателя, се получават успешно. Загубите се дължат на факта, че за тази скорост устройството вече е напуснало мрежовия обхват и не е получило останалите пакети. С увеличаване на скоростта се забелязват все повече неправилно получени или неполучени данни.
Резултатите показват, че с увеличаване на скоростта на движение на потребителското устройство и разстоянието между приемника и предавателя процентът на погрешно приетите символи се увеличава. Скоростта, с която няма грешки по време на предаването в тази тестова Li-Fi мрежа, е 1m/s.

B.4.6. Haka, V. Aleksieva and H. Valchanov, "Enhanced Simulation Framework for Visualisation of IEEE 802.15.4 Frame Structure on Beacon Enabled Mode of ZigBee Sensor Network," 2020 International Conference on Biomedical Innovations and Applications (BIA), Varna, Bulgaria, 2020, pp. 109-112, doi: 10.1109/BIA50171.2020.9244507.

Този доклад представя подобрения в симулационния продукт за ZigBee за IoT, предложен от авторите в предишно изследване. Основните подобрения на симулационния софтуер са: възможност за изчисляване на стойностите за Received Signal Strength (RSS) и Received Signal Strength Indicator (RSSI); визуализиране на съдържанието на кадъра IEEE802.15.4 в beacon-enabled режим; изучаване на класически алгоритми за приоритизиране на трафика в сензорни мрежи; проучване на параметри, влияещи на QoS, като Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), забавяне и пропускателна способност.
Като подобрение на симулационния продукт за мрежата ZigBee е внедрен един Knowledge Free и един Knowledge Based алгоритъм за приоритизиране на мрежовия трафик. Knowledge Free алгоритмите обработват заявките по реда на тяхното пристигане. Такъв алгоритъм за приоритизиране на трафика е First Come First Served (FCFS). Knowledge Based алгоритмите използват или информация за приложението, или информация за мрежата или и двете, за да дадат приоритет на трафика. Реализираният алгоритъм Least Number of Hops First (LNHF) се основава на познаване на мрежовата информация. Според този алгоритъм заявките от устройствата по-близо до координатора се обслужват с висок приоритет. Изграждането на ZigBee мрежа се осъществява с помощта на графичен потребителски интерфейс, чрез който се създават координаторите и към тях се добавят крайни сензорни възли. Параметри като: брой на свързаните крайни възли, честотна лента на канала, област, честота, ред на beacons и ред на суперкадри се задават за всеки PAN координатор. За да се уточни и свърже създадената симулация с ограниченията за определен регион в света, е добавена опция за избор на определен канал и визуализиране на работната честота.
Когато координаторът и крайните възли са правилно добавени със съответната конфигурация, трафикът, генериран от крайните възли в мрежата, се приоритизира. При приоритизиране на трафика според избрания алгоритъм се попълва съдържанието на пет IEEE 802.15.4 кадъра.
Резултатите за статични възли от проведените тестове показват, че алгоритъмът LNHF подобрява QoS за крайните възли, на разстояние до 7 м от обслужващото устройство. Това ще ускори работата, тъй като смущенията в тези възли са по -малко, тъй като сигналът от координатора е по -добър, съответно препредаването на пакети ще бъде по -малко.
Резултатите от тестовете с мобилни възли за разглежданите алгоритми за приоритизиране са подобни. За устройствата, движещи се със средна скорост, разпределените ресурси са малко и разглежданите стойности се влошават. Това може да влоши QoS за тези устройства, тъй като обработката на техните заявки ще бъде забавена, а допълнително забавяне ще бъде причинено от иницииране на предаване, когато устройството е извън обхвата на текущия координатор.

B.4.7. Haka, V. Aleksieva, H. Valchanov and D. Dinev, "Analysis of ZigBee Network Using Simulations and Experiments", 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-4, doi: 10.1109/ICAI50593.2020.9311328.

Този доклад сравнява резултатите за стойностите на Received Signal Strength Indicator (RSSI) от възлите на крайните сензори, получени чрез симулиране на мрежа ZigBee, използвайки подобренията на симулационния продукт, представени в B.4.6. и чрез истинска сензорна мрежа ZigBee. Графичният потребителски интерфейс на симулатора позволява добавяне на координатори и крайни сензорни възли за изграждане на мрежа ZigBee. След като са добавени ZigBee PAN координатори, крайните сензорни възли могат да бъдат свързани към тях. Стойностите за RSS и RSSI се изчисляват веднага след задаване на разстоянието на сензора от координатора. Промените за всички въведени параметри се отразяват в таблиците с данни и могат да бъдат проверени от раздела „Nodes Table". Симулаторът изчислява автоматично стойностите за RSS и RSSI, въз основа на разстоянието между добавените крайни сензори и PAN координатора. Изчислените стойности, са представени с графики според разстоянието на възела до PAN или идентификатора на възела.
Тестовете за RSS и RSSI от симулатора бяха получени след изграждане на мрежа ZigBee от един координатор (маршрутизатор ZigBee) и 6 сензорни възела ZigBee, свързани в топология „звезда".
Физическото изграждане на мрежата ZigBee се осъществява с платка BeagleBone Black-BBB01-SC-505 с операционна система Bone-Debian-7.8, работеща като ZigBee Gateway, трансивер Texas Instruments (TI)-CC2531EMK и TI мулти-стандартни сензорни възли-CC2650STK. ZigBee Gateway е конфигуриран с помощта на TI Z-Stack Linux Gateway. Платката CC2531EMK е конфигурирана да работи като трансивер ZigBee и сензорните възли за работа в мрежата ZigBee, използват CC-DEVPACK-DEBUG на TI. Прехвърлянето на данни и получаването на RSSI стойности от крайните сензорни възли във вече изградената мрежа ZigBee може да бъде проследено, когато втори трансивер CC2531EMK е конфигуриран да работи като ZigBee sniffer. Резултатите за получените RSSI стойности от изградената мрежа ZigBee са противоречиви при тестовете за 2, 4 и 6 сензорни възли. Резултатите от 2 сензора показват, че с увеличаване на разстоянието от координатора получените RSSI стойности се влошават. Тази тенденция не се наблюдава при тестовете с 4 и 6 сензорни устройства. В тях, с увеличаване на разстоянието от координатора, получените RSSI стойности са идентични или по -добри за някои от възлите и по -лоши за други. Това се дължи на наличието на външни шумови влияния и смущения между сензорните възли, които могат да се увеличат с броя на устройствата в мрежата. Получените резултати показват, че за 2 крайни устройства в мрежата стойностите за RSSI, получени чрез симулатора, са почти идентични с тези за тестовете с реална мрежа. Резултатите с 4 и 6 крайни устройства, получени чрез симулатора, са близки до тези на реалната мрежа. Отклонението в RSSI стойностите на симулатора е около 10dB в сравнение с действителните резултати.

B.4.8. D. Dinev, V. Aleksieva and H. Valchanov, "Simulation Framework For Studying Quality of Service Traffic Prioritization Algorithms in Li-Fi Network", 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-4, doi: 10.1109/ICAI50593.2020.9311358.

Този доклад представя симулационен софтуер за изучаване на алгоритмите за QoS приоритизация на трафик в Li-Fi мрежи. В него са внедрени алгоритъм, предложен от авторите от предишни изследвания, алгоритъм за приоритизиране на трафика на Wang и два класически алгоритма - First Come First Served (FCFS) и Least Number of Hops First (LNHF). Симулаторът изчислява packet delivery ratio (PDR), packet loss ratio (PLR), пропускателна способност и закъснение въз основа на разпределението на ресурсите чрез внедрените алгоритми.
Предложената стратегия за приоритизиране на трафика разпределя ресурсите в рамките на един времеви интервал, като отговаря на някои критерии. Пренареждането на потребителите, свързани към терминала според алгоритъма на авторите, е следното: потребителите, които са по -близо до него, имат по -висок приоритет и отиват по-високо в таблицата на потребителите. Ако разстоянието от терминала до някои от потребителите е равно, тогава алгоритъмът търси следващи критерии - клиентското устройство мобилно или статично е? Статичните устройства имат по-малък приоритет. Мобилните потребители имат по-висок приоритет според скоростта си. Колкото по-висока е скоростта, толкова по-висок приоритет има устройството. Видът на исканата услуга е последният критерий на алгоритъма. Всеки от тях принадлежи към определен клас, който има различен приоритет според QoS параметрите. Има четири вида класове:
• Клас 1 - съдържа услуги за хендовер между клетки, повиквания за възстановяване на връзки и гласови повиквания.
• Клас 2 - съдържа услуги на видео повиквания.
• Клас 3 - съдържа услуги за предаване, HDTV и гласови съобщения.
• Клас 4 - съдържа само услуги за фонов трафик.
Новата функционалност включва възможност за приоритизиране на свързани потребители чрез внедряване на нови алгоритми, изчисляване на техните QoS параметри за PDR, PLD, закъснение и пропускателна способност, сравняване на параметрите по всеки алгоритъм и показване на предавателната матрица за всеки алгоритъм. Предавателната матрица за всеки алгоритъм може да бъде показана след изчисляване и разпределение на ресурсите, поискани от свързаните устройства. Добавена е нова таблица с данни за съхраняване на параметъра QoS за всеки алгоритъм. За лесно сравняване и проучване на QoS параметрите за всеки алгоритъм може да се направи графична диаграма за всеки от тях.
Софтуерът реализира напълно работеща симулация на Li-Fi мрежа с терминални устройства и свързани с тях потребители с техните спецификации. Съгласно реализирания алгоритъм за приоритет на трафика и разпределение на ресурсите, софтуерът може да изчисли PDR, PLD, закъснение и пропускателна способност, които са важни за осигуряване на по-добро качество на услугата.
Според тези резултати може да се направи заключението, че алгоритъмът, който се предлага, има по-добри стойности на QoS от останалите, разгледани в тази статия.

B.4.9. Aydan Haka, Veneta Aleksieva, Hristo Valchanov, 6LoWPAN Network Analysis Using Simulations and Experiments, IOP Conference Series: Materials Science and Engineering, CIEES'20, vol. 1032 (2020), pp.1-4, doi:10.1088/1757-899X/1032/1/012015, ISSN: 1757-8981, https://iopscience.iop.org/article/10.1088/1757-899X/1032/1/012015

Този доклад представя физическо реализиране на 6LoWPAN мрежа и изследване на показателите за пропускателна способност от край до край, което се сравнява с резултатите, получени чрез симулационния продукт 6LoWPAN, представен в предишни изследвания на авторите. Тестовете за пропускателна способност и закъснение от край до край от симулатора бяха получени след изграждане на мрежа 6LoWPAN от един координатор и 6 сензора 6LoWPAN, свързани в топология „звезда". Координаторът е конфигуриран да работи по канал 25. До 6 крайни сензорни възела 6LoWPAN могат да бъдат свързани към координатора. Всички крайни възли са статични, изпълняват един и същ тип приложение и се намират на еднакво разстояние от координатора (от 1м до 5м). Тестовете за отчитане на стойностите за пропускателна способност и закъснение от край до край са направени с 2, 4 и 6 сензорни възли, свързани към 6LoWPAN координатора. След като се добави информация за координатора и крайния възел, се извършва симулация за изпращане на определен брой пакети. След добавяне на пакетите към опашката за изпращане се изчисляват стойности за закъснение от край до край и пропускателна способност. Резултатите от проведените експериментални проучвания са голям брой, затова те са обобщени и представени в таблица. Тъй като симулаторът представя експериментите в идеални условия, на различни разстояния получените стойности са идентични. Разликата в проведените експерименти се получава от различния брой изпратени пакети.

Физическото изграждане на 6LoWPAN мрежата се осъществява с платка BeagleBone Black-BBB01-SC-505 с операционна система Bone-Debian-9.9, работеща като 6LoWPAN Gateway, TI трансивер-CC2531EMK и TI мулти-стандартни сензорни възли- CC2650STK. Прехвърлянето на данни и броя на битовете за получаване от крайните сензорни възли във вече изградената 6LoWPAN мрежа могат да бъдат проследени, когато втори трансивер CC2531EMK е конфигуриран да работи като 6LoWPAN снифер. Това е направено на Linux машина с помощта на програмата Sensniff за 6LoWPAN.

Експериментите са направени с 2, 4 и 6 сензора със симулатор и с реална мрежа при еднакви условия. Например, отклонението в симулираните резултати с 6 сензора от реалните за закъснение от край до край е средно 99% за 5, 10, 15 и 20 изпратени пакета, а за пропускателната способност е 98% за 5 пакета, 94% за 10 пакета, 86% за 15 пакета и 79% при 20 пакета. Резултатите от тестовете в реална мрежа са променливи, тъй като комуникацията между сензорите и координатора се влияе от фактори на околната среда като електромагнитни смущения, радиосмущения, грешки при предаване на пакети, други източници, работещи на същата честота, смущения между сензори и др.

Получените тенденции в резултатите от симулацията и реалната мрежа се доближават, което дава основание да се твърди, че симулационният продукт е подходящ за образователни цели.

B.4.10.Aydan Haka, Veneta Aleksieva, Hristo Valchanov, Deployment and Analysis of Bluetooth Low Energy Network, IOP Conference Series: Materials Science and Engineering, CIEES’20, vol. 1032 (2020), pp.1-4, doi:10.1088/1757-899X/1032/1/012016, ISSN: 1757-8981, https://iopscience.iop.org/article/10.1088/1757-899X/1032/1/012016

Този доклад представя реализирането на физическа Bluetooth ниско енергийна (BLE) сензорна мрежа за IoT и изследване на RSSI стойностите, получени за крайните сензорни блокове в мрежата. Физическото изграждане на BLE мрежата е направено с платка RaspberryPi 4 Model B с операционна система Raspbian, работеща като BLE master устройство, с вграден BLE трансивър и многостандартни сензорни възли на Texas Instruments-CC2650STK. Топология “звезда” е реализирана чрез свързване на крайните сензорни възли и master-а за изследване на промяната в RSSI стойностите. Извършени са различни експерименти с 1, 2, 3, 4, 5 и 6 статични възли, където за всеки от тях възлите са разположени на разстояния от 1 м до 10 м от главното устройство. Извършено е изследване на промените в получените RSSI стойности за статични сензори, разположени на различни разстояния от главното устройство и за мобилни възли, движещи се с различни скорости.

За 1 възел резултатите показват, че с увеличаването на разстоянието на сензора от главното устройство, получените RSSI стойности се влошават. Стойността на 10 метра обаче е значително по-добра от предишните. Въпреки че само едно устройство предава в комуникационната среда, която не е натоварена, спадът на предишните стойности може да се дължи на външни източници на смущения. Тенденцията, че на по-близко разстояние до обслужващото устройство получените RSSI стойности са по -добри, се потвърждава от другите тестове с 3, 4, 5 и 6 сензора. Измерените стойности за RSSI намаляват все повече и повече, когато разстоянието от главното устройство и броя на крайните възли в мрежата се увеличават. Подобни експерименти са проведени и с мобилни възли. За втория възел се вижда, че стойностите за RSSI са значително по-ниски. Това се поражда от натоварването на комуникационната среда и възникналите смущения. Тенденцията, когато сензорите се движат с по-ниска скорост, получените RSSI стойности са по -добри, се потвърждава от другите тестове с 3, 4, 5 и 6 сензора. Експерименталните резултати за RSSI със статични сензорни възли показват, че с увеличаване на разстоянието между крайните възли и главното устройство, получените стойности се влошават със значителни промени. Експерименталните резултати за RSSI с мобилни сензорни възли показват, че с увеличаване на скоростта на крайните възли получените стойности се влошават, но промяната в резултатите е по-плавна.

Както за статични, така и за мобилни възли се запазва тенденцията за влошаване на RSSI стойностите с увеличаване на броя крайни сензорни възли в мрежата.

B.4.11.A. Haka, V. Aleksieva and H. Valchanov, "Simulation Environment for Research of Algorithms for Traffic Prioritisation in ZigBee Network," 2021 17th Conference on Electrical Machines, Drives and Power Systems (ELMA), 2021, pp. 1-4, doi: 10.1109/ELMA52514.2021.9503088.

Този доклад представя симулационна среда, която позволява да се проучи влиянието на внедрените алгоритми за приоритизиране на трафика върху параметри, свързани с качеството на услугата (QoS) в мрежата ZigBee. Предложеният алгоритъм за приоритизиране на трафика за ZigBee е модификация на предходен предложен от авторите алгоритъм и е предназначен да работи в топология „звезда“. Подобренията на продукта са способността да се изследва влиянието на различни алгоритми за приоритизиране на трафика върху параметри, тясно свързани с QoS, както и визуализация на изградената топология на мрежата. Симулационният продукт има модулна архитектура, а работата на отделните модули се контролира от ядрото му. Алгоритъмът проверява няколко критерия за приоритизиране на трафика в мрежа ZigBee. Първо се проверява за пакети, които са маркирани като спешни. При наличието на такива пакети те се обслужват с най-висок приоритет. Когато има няколко спешни пакета или те липсват, трафикът се приоритизира според това дали заявката е от мобилно или статично устройство. Заявките от мобилни устройства се обслужват с по-висок приоритет. Когато има пакети от повече от едно мобилно устройство, заявките се приоритизират според скоростта, с която се движат устройствата. Заявките с по-висок приоритет се обслужват от устройства, които се движат по-бързо. Друг критерий за приоритизиране при равни други условия е разстоянието на сензора от координатора. Заявките от сензори, по-близки до координатора, се обслужват с по-висок приоритет. Когато сензорите са на равно разстояние от координатора, техните заявки се приоритизират според стойността на cost. Заявки с по-висока стойност на cost се обслужват с по-висок приоритет. И накрая, заявките се приоритизират според приложението на сензора.
Извършените експерименти имат за цел да проучат влиянието на внедрените алгоритми за приоритизиране на трафика в мрежата ZigBee върху параметрите PDR, PLR, закъснение и пропускателна способност, които са важни за осигуряване на добро QoS. Представените експериментални резултати показват, че с увеличаване на броя възли услугата на предложения алгоритъм за приоритизиране на трафика в мрежата ZigBee става равномерна. За изследваните параметри обаче са предвидени по-високи стойности за по-близките до координатора възли. Това ще подобри QoS и ще ускори обслужването за тези устройства. Това ще освободи по-бързо заетия ресурс и ще позволи по-бързо да се обслужват заявките с най-нисък приоритет от най-отдалечените устройства.
Обратно, услугата на класическите алгоритми е значително равномерна, което натоварва цялата комуникация в мрежата и може да доведе до влошаване на QoS. В допълнение, предоставянето на повече ресурси от предложения алгоритъм за обслужване на заявки от възли с по -висок приоритет, за разлика от класическите, ще удължи живота им на батерията, тъй като консумацията на енергия е само в активни периоди, а броят им може да бъде сведен до минимум чрез ускоряване на обслужването.

B.4.12.Aydan Haka, Diyan Dinev, Veneta Aleksieva, Hristo Valchanov, Comparative analysis of ZigBee, 6LoWPAN and BLE technologies for the Internet of Things, AIP, CIEES’21,25-27.11.2021, Rouse, Bulgaria (приета)

Този доклад представя реализацията на сензорна мрежа за IoT със сензори Texas Instruments CC2650STK, които могат да бъдат конфигурирани да работят с ZigBee, 6LoWPAN и BLE технологии. Извършени са експериментални проучвания на параметрите End_to_End Delay, Throughput и PLR за трите технологии. Въз основа на резултатите от експериментите е представено сравнение на същите между разглежданите технологии. Целта е в резултат на изследването да се формулират препоръки за най -подходящата технология за изграждане на сензорна мрежа за IoT с използваните сензорни възли.
Експерименталните изследвания за разглежданите технологии се реализират с различен брой едновременно свързани в мрежата статични сензорни възли (2, 4 и 6). Експериментите включват изчисляване на стойностите на параметрите End_to_End Delay, Throughput и PLR, които влияят на QoS, на разстояния между обслужващото устройство и сензорните възли от 1m, 2m, 3m, 4m и 5m, при изпращане на 5, 10, 15 и 20 пакета. За да се осигури сравнимост между получените резултати за изследваните технологии, във всички експерименти е използвана топология „звезда“.
Според получените резултати стойностите за End_to_End Delay се увеличават с броя на крайните възли в разглежданите технологии, тъй като е необходимо повече време за обслужване на заявките на всички устройства. С увеличаването на броя на изпратените пакети се увеличават и стойностите, получени за End_to_End Delay, тъй като има повече заявки за обслужване в мрежата. При ZigBee в повечето експерименти минималната и максималната стойност за End_to_End Delay е по -добра от 6LoWPAN и BLE. Освен това в повечето експерименти получените стойности за ZigBee са постоянни и не се променят драстично с увеличаване на разстоянието между крайните възли и обслужващото устройство.
От получените резултати за PLR може да се види, че стойностите се увеличават правопропорционално на броя на възлите в мрежата за разглежданите технологии.
Следните препоръки могат да бъдат формулирани от експериментите и получените резултати:
• В приложения, където е важно стойностите за End_to_End Delay да са относително ниски и постоянни е по -добре сензорните възли CC2650STK да бъдат конфигурирани да работят с технологията ZigBee;
• В приложения, където се изискват постоянна throughput е по -добре сензорните възли CC2650STK да бъдат конфигурирани да работят с технологията ZigBee;
• Когато се изисква да се осигури по-висока производителност с по-голям брой възли в мрежата е по-добре сензорните възли CC2650STK да бъдат конфигурирани да работят с BLE технология;
• В приложения, където се изисква по-малка загуба на пакети, е по-добре сензорните възли CC2650STK да бъдат конфигурирани да работят с ZigBee или BLE технология, тъй като получените PLR стойности са изключително близки, но с по -ниски стойности, получени за ZigBee.

B.4.13. A. Haka, Y. Yordanov, V. Aleksieva and H. Valchanov, "Simulation Environment for Bluetooth Low Energy Network," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 287-290, doi: 10.1109/ICAI52893.2021.9639521.

В днешно време с разширяването и усъвършенстването на комуникационните технологии предлаганите услуги се увеличават, като например технологии за широколентов интернет на нещата (IoT), а една от най-разпространените IoT технологии е Bluetooth Low Energy (BLE).
Този доклад представя симулационен продукт за изследване на комуникацията и съобщенията между Master и Slave в мрежата BLE, който може да се използва и в образованието. Може да се използва както за изучаване на основните функционалности на технологията, така и по време на обучение на място или онлайн.
Разработеният симулатор в катедра КНТ към Технически университет - Варна е с модулна архитектура. При зареждане на приложението се стартира основната функционалност на ядрото, която е добавяне на Master устройството и реализиране на неговата програмна логика за обработка на входящите пакети и съответния им тип PDU, както и изчакване за добавяне на Slave устройство и наблюдение на състоянието му (Standby, Advertising, Connected). Изпълнението на основната функционалност се контролира от класа "AppController".
За да се получи статистическа информация за времето, през което крайните устройства в мрежата са били в определено състояние, ядрото се обръща към модула за статистика, който се управлява от класа „DeviceStatisticsUtil“. Обработената информация чрез различните модули се визуализира чрез изградения графичен потребителски интерфейс (GUI).
След добавяне на Slave устройства, на всяко от тях може да се позволи да визуализира разстоянието до Master, да бъде премахнато от мрежата или да промени статуса му от Standby на Advertising.
Когато състоянието на Slave е Advertising, то започва да изпраща рекламни пакети по предназначените за това канали (37, 38 и 39). С това Slave изпраща броадкастни пакети в комуникационната среда, така че да може да бъде открито от Master в обхвата му и евентуално да се свърже с него. При преминаване към Advertising режим също започва проследяване на пакетите, предавани през комуникационната среда.
За да се сравни обменът на съобщения при установяване на връзка, изпращане на данни и прекратяване на връзката между Master и Slave устройства в BLE симулатора и реална среда, се конфигурира истинска BLE мрежа. За да се осигури сравнимост между резултатите от реалната и симулирана BLE мрежа, е реализирана експериментална топология от един Master и един Slave.
По време на симулацията някои от детайлите на комуникацията са пропуснати, за да се опрости разглежданият процес и да се улесни представянето му по време на обучението.
Симулаторът представя основните съобщения в изпълнението на процеса, което му позволява да се използва по време на обучението както на място, така и онлайн. Резултатите показват, че симулаторът може да се използва за представяне на акцентите в комуникацията между Master и Slave.

B.4.14. D. Dinev, V. Aleksieva, H. Valchanov and K. Genov, "Simulation Software For Finding Best Route in LoRaWan Network," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 291-294, doi: 10.1109/ICAI52893.2021.9639718.

LoRaWan е с дълъг обхват, ниска мощност, нискоскоростна, безжична телекомуникационна система, популяризирана като инфраструктурно решение за IoT: крайните устройства използват LoRaWan чрез един безжичен gateway, свързан с Интернет. Той работи като прозрачен мост и предава съобщения между тези крайни устройства и централен мрежов сървър.
Тази статия представя симулационен софтуер за намиране на най-добрия маршрут в LoRaWan мрежи.
Depth First Search е алгоритъм за обхождане или търсене в структури от данни като "дърво" и "граф". За да се приложи алгоритъмът, се избира връх или възел на структурата, който се обозначава като корен и обхождането започва от него. Всички следващи върхове се посещават последователно в дълбочина до достигане на един, без наследници, след което се извършва търсене с връщане назад до достигане на нова крайна точка или след пълното обхождане - до корена. Оригиналната версия на алгоритъма е създадена през 19 век от Шарл Пиер Тремо за решаване на проблеми с лабиринта.
Симулаторът използва модифицирана версия на алгоритъма, който търси всички пътища само до едно крайно устройство, дефинирано като дестинация, за да намери всички възможни маршрути от определена частна локална мрежа към друга мрежа.
В мулти-хопови мрежи може да има няколко маршрута с еднакви параметри. Първоначално с помощта на Hassle Free Route маршрутът се избира според параметъра за най-кратък път. Включена е уникална стойност, за да се даде приоритет на маршрутите. Уникалната стойност се съхранява в таблиците за маршрутизиране на устройствата като отрицателно, положително число или 0, където:
• отрицателно число - има голяма загуба на пакети по маршрута;
• положително число - маршрутът е добър;
• 0 - стойност по подразбиране; маршрутът не е оценен.
По-високата положителна стойност показва, че маршрутът е по-добър от останалите. Тя показва броя на успешните предавания по този маршрут. За всяко успешно предаване тази стойност се увеличава с 1, а за всяко неуспешно предаване се намалява с 1. Когато фрагмент съдържа emergent dispatch header, той се препраща към маршрута с най-високата уникална стойност. Тези фрагменти се приоритизират и изпращат по най-предпочитания път.
Средното време за изпращане на 51-байтов LoRaWan фрагмент е Ttrans = 6 ms, което включва времето за предаване и back-off таймера.
Симулаторът има 5 основни модула - GUI, Core, Creating topology, Topology modification, Finding best path between end devices.
За да се направи тест за намиране на „Най -добър маршрут“ между крайни устройства, е симулирана LoRaWan мрежа с 5 терминални и 4 крайни устройства.
Направени са тестове за намиране на най-добрия маршрут между крайни устройства и е доказано, че предложеният симулатор е напълно функционален и подходящ за изследвания на LoRaWan мрежи.

B.4.15. D. Dinev, V. Aleksieva and H. Valchanov, "Comparative Analisis of Li-Fi Simulators for Purposes of the Education," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 125-128, doi: 10.1109/ICAI52893.2021.9639691.

Li-Fi технологията за Internet of Things осигурява висока скорост, двупосочен и сигурен безжичен достъп. Това изисква проучване на качеството на услугата на тази технология. Това може да стане с помощта на симулационен софтуер, който ще намали разходите и времето за изграждане на такива мрежи. Тази статия представя информация за сравнителен анализ между предложения от авторите в предишни доклади симулатор и някои от най-известните симулатори (OptSim, Veins VLC, NS-2, NS-3, MATLAB) за изследване на качеството на услугата в Li-Fi мрежи. Предложена е система от критерии за извършване на сравнителен анализ на симулатори за Li-Fi мрежата. Този подход към изследванията на Li-Fi мрежата за IoT може да бъде въведен и в образованието.

Съществуващите симулатори на Li-Fi мрежи имат редица недостатъци, свързани с тяхната работа и функционалност. Тук те са представени.

Предложените критерии за сравнение на симулаторите LiFi са:

• Моделиране на различни алгоритми за приоритизиране на трафика в LiFi
• Моделиране на различни методи за разпределение на ресурси
• Симулация на мобилност
• Поддържане на GUI
• Визуално представяне на изследваната мрежа
• Анализ на получените резултати
• Лесен монтаж
• Мащабируемост
• Ръководство на потребителя/разработчика
• Програмен език
• Използване на паметта
• Лиценз за използване

Според представените резултати от изследването, поради широкия спектър от разглеждани критерии, най-подходящи за изследване на Li-Fi мрежи са MATLAB, OptSim и NS-3. Отделно проучване на критериите обаче показва, че предложеният от авторите симулатор осигурява по-добри стойности за показателите: „Лесна инсталация", „Използвана памет" и „Лиценз за използване", които са изключително важни за образователни цели.

Критериите за сравнение не определят критериите "Визуализация на матрицата на предаване", т.е. за разлика от симулатора, предложен от авторите, никой от другите симулатори не предоставя тази възможност. Той осигурява сравними, с други симулатори, резултати спрямо много други критерии. Това доказва, че авторският симулатор е много подходящ за обучение и образователни цели.

B.4.16. A.Haka, V. Aleksieva and H. Valchanov, "ZigBee Simulation Framework for Studying the Formation of a Hierarchical Tree Topology," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 257-260, doi: 10.1109/ICAI52893.2021.9639563.

ZigBee е една от модерните технологии за управление на IoT сензорни мрежи, тъй като осигурява високо качество на обслужване (QoS) и ниска консумация на енергия. Едно възможно решение за постигане на по-добър QoS в тези мрежи е да се използва ефективен алгоритъм за маршрутизиране на трафика. Тази статия представя подобрен симулатор, в който е реализиран алгоритъм за формиране на йерархична топология на ZigBee, базиран на приоритети, позволяващ йерархично маршрутизиране. Симулаторът предоставя възможност за анализ на резултатите от алгоритъма чрез визуална интерпретация на мрежовата топология.
ZigBee използва смесен механизъм за маршрутизиране, комбиниращ hierarchical tree routing protocol (HRP) и ZigBee ad hoc on-demand distance vector (Z-AODV). HRP е активен метод за маршрутизиране, чиято информация за маршрута се установява, когато мрежата е разгърната и остава непроменена, освен когато се промени структурата на мрежата.
В симулатора е приложен алгоритъмът на авторите за формиране на енергийно балансирана мрежа ZigBee въз основа на приоритети с дървовидна топология. Топологията ZigBee се състои от един координатор (коренът на дървото), множество маршрутизатори (клонове) и крайни устройства (листа). В този алгоритъм методът на ценообразуване се използва за постигане на целта. В алгоритъма се приема, че рутерите служат само за изграждане на топологията и не функционират като крайни устройства. Всеки рутер и крайно устройство имат готовност да плащат стойност - приоритет за крайните устройства и ниво на енергия за рутерите. Координаторът и маршрутизаторите имат стойност на таксуване - цена, която трябва да бъде платена от крайните възли, за да се свържат с тях. Следователно, колкото по-висока е стойността на готовността за плащане, толкова по-висок е приоритетът на крайното устройство. При рутерите случаят е подобен, колкото по-висока е стойността на готовността за плащане, толкова повече енергия имат.
Симулаторът има модулна архитектура. Симулирането на ZigBee мрежа изисква работа през два основни прозореца. Единият от тях за добавяне на параметри за координатора, а другият за маршрутизаторите и крайните възли в мрежата.
Визуализацията на топологиите от проведените експерименти за внедрения алгоритъм за формиране на йерархична топология в мрежата ZigBee показва, че с увеличаване на броя на рутерите дълбочината на йерархията в изграденото дърво се увеличава. По отношение на енергийния баланс, алгоритъмът за формиране на йерархията гарантира, че рутерите с повече енергия са подредени на по-ниско ниво (по-близо до координатора). Това осигурява по-добра енергийна ефективност на рутерите, тъй като повече устройства ще бъдат свързани към тези с повече енергия и по-малко устройства към тези с по -малко енергия.
Експериментите показват, че внедреният алгоритъм позволява изграждането на балансирана по отношение на енергийната ефективност йерархична топология.

Г. Публикации извън групата на монографичния труд
Г.7. Публикации в реферирани и индексирани в световноизвестни бази данни с научна информация

Г.7.1. Veneta Aleksieva, Hristo Valchanov and Anton Huliyan, Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services, 8-9.11.2019, Varna, BIA 2019, p. 69-72, ISBN 978-1-7281-4754-3, IEEE Catalognumber: CFP19U85-ART, DOI: 10.1109/BIA48344.2019.8967468

Този доклад представя експериментално внедряване на интелигентни договори за застрахователни услуги, базирани на Ethereum блокчейн. Реализиран е децентрализиран крипто-жетон, базиран на стандарта ERC20 за интелигентен договор. Създаден е уеб-базиран интерфейс за продажби на тези крипто-токени. Представени са резултатите от експерименталните тестове.
Класическият процес на заявяване на щета може да бъде подобрен чрез използване на интелигентни договори и блокчейн технология. Информацията за щетата може да бъде изпратена от застрахования или директно от сензори, монтирани в обекта на застраховка (интелигентен актив) до автоматизираното приложение за обработка на искове. За съответните застрахователни полици, предоставени от интелигентния договор, клиентът ще получи потвърждение в реално време. Искът се обработва автоматично чрез интелигентен договор въз основа на бизнес логика, като се използва информацията, предоставена от застрахователя.
Този подход автоматично използва допълнителни източници (статистика, отчети) за оценка на претенциите и за изчисляване на загубите. В зависимост от застрахователната полица, интелигентният договор може автоматично да изчисли личната отговорност. В определени ситуации интелигентният договор може да активира допълнителна оценка на иска. Ако искът е одобрен, плащането към застрахования се инициира чрез интелигентен договор.
Предимствата на новия подход, базиран на интелигентни договори за блокчейн технологията, могат да се видят в няколко аспекта. Подаването на искове е опростено и автоматизирано. Благодарение на директния обмен на информация за щети между застрахователите, този подход елиминира нуждата от брокери и намалява времето, необходимо за разглеждане на исковете. Вградената бизнес логика в интелигентния договор за блокчейн елиминира необходимостта от регулатор на загуби за преразглеждане на всяка претенция (освен в конкретни ситуации). Застрахователят има достъп до произхода на щетата, което му помага да идентифицира потенциални опити за измама. Процесът на плащане на щета е автоматизиран от интелигентния договор на блокчейна, без да е необходим посредник за заявяване на искове.
Предложеното решение с интелигентни договори за застраховки се основава на стандарта ERC20. Той е внедрен експериментално на Ethereum блокчейн. Резултатите от експериментите показват, че предложеното решение е напълно работоспособно по отношение на управление на автоматичните плащания по одобрени претенции за загуба.

Г.7.2. V. Aleksieva, H. Valchanov and A. Huliyan, "Implementation of Smart-Contract, Based on Hyperledger Fabric Blockchain", 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), Bourgas, Bulgaria, 2020, pp. 1-4, doi: 10.1109/SIELA49118.2020.9167043.

Докладът представя решение за създаване на интелигентен договор, базиран на Permission блокчейн, конкретно- Hyperledger Fabric.
Предложеният смарт-договор е реализиран на компютър с AMD Ryzen 5 2600 с 6 ядра/12 нишки, 3.4GHz, 16GB DDR4 3200Mhz и SSD Nvme 500GB, скорост на четене/запис 3500/2700 MB/s. Операционната система е Linux Ubuntu 16.04 LTS 64bit. Освен това се използват Docker Engine версия 17.03 и Docker-Compose версия 1.8.
Топологията на Blockchain мрежата е следната: Има една компания (R1), която има един order възел (O1) и един peer възел (P1). Работи с две различни компании - R2 и R3. Всеки от тях има собствен консорциум с основна компания. Те се реализират в два независими канала - C1 и C2. Всеки консорциум има два peers - C1 има P3 и P1, C2 има P2 и P1. Тъй като peer P1 работи за основната компания R1, той участва в два канала. L1 е копие на Blockchain на C1, L2 е копие на Blockchain на C2.
Бизнес решението, базирано на блокчейн, се реализира чрез осигуряване на връзка между отделните организации за съхранение и обмен на информация, както и за нейната обработка. Данните са видими само между организациите, които имат права на достъп, за които между тях са създадени канали за комуникация. За да се поддържа коректността на данните по време на запис и съхранение, пиърите се конфигурират в рамките на организацията, за да поддържат работоспособността на мрежата.
Блокчейн мрежата използва Docker контейнер за внедряването на Hyperledger Fabric. Той използва инструмента Docker Compose за определяне и изпълнение на многоконтейнерни приложения на Docker.
След като блокчейн мрежата е конфигурирана и стартирана, бизнес логиката, която ще се изпълнява в нея, трябва да бъде внедрена. Интелигентните договори (codechains) се създават с езика за програмиране Go.
Тестовете са представени с Hyperledger Explorer за Fabric 1.4.x под Linux Ubuntu. Предложеното решение позволява бърза и сигурна миграция на интелигентни договори между независими канали. Всеки канал има собствена бизнес логика и е невидим за участниците в други канали.

Г.7.3. V. Aleksieva, H. Valchanov and A. Huliyan, "Implementation of Smart Contracts based on Hyperledger Fabric Blockchain for the Purpose of Insurance Services", 2020 International Conference on Biomedical Innovations and Applications (BIA), Varna, Bulgaria, 2020, pp. 113-116, doi: 10.1109/BIA50171.2020.9244500.

Докладът представя внедряване на интелигентни договори за застрахователни услуги на собственост, базирани на Hyperledger Fabric Blockchain. Частната блокчейн като Hyperledger Fabric Blockchain е по-добро решение за застрахователния бизнес, защото работи върху доверени устройства (nodes), не се налага изискване за протокол за консенсус. Основните предимства са бързият достъп до информация, по-евтините транзакции и контролът на ниво поверителност. Поради тези факти този блокчейн е подходящ и полезен в много области на застрахователните услуги.

В представения случай на използване се създават два канала: един за консорциум 1 (Channel 1) на компания Org1 (застрахователна компания) и компания Org2 (брокер 1), и един за консорциум 2 (Channel 2) на компания Org1 и компания Org3 (брокер 2). Всеки канал има свой собствен блокчейн, както и интелигентни договори (codechain), които работят самостоятелно с него. Всеки консорциум има двама участници. Двата канала работят паралелно и не са видими за участниците извън разрешените от правилата на консорциума. Един peer може да съдържа копие от блокчейна и интелигентни договори на повече от един канал.

Предложеният умен договор (codechain) е реализиран на компютър с AMD Ryzen 5 2600 6 ядра/12 нишки, с Linux Ubuntu 16.04. Освен това се използват Docker Engine версия 17.03 и Docker-Compose версия 1.8. Името на създадения интелигентен договор е *mycc* и е инсталиран на Peer 0 на Org1 в Channel 1. Съгласно внедрената бизнес логика е възможно клиентът да смени своя брокер. Това означава, че неговата полица трябва да се премести от един канал в друг канал. Има два възможни сценария, след като се копира - той да остане видим в channel 1, а промените, направени след копирането в channel 2, няма да бъдат видими. Другият сценарий е, че той ще бъде изтрит, така че вече няма да се вижда за участниците в channel 1.

Тестването на работоспособността на случая на използване се извършва чрез изпращане на заявки до инсталираните codechains и проверка на правилното им изпълнение. Инструментът Hyperledger Explorer се използва за визуализиране на създадената мрежа за този експериментален случай на използване. За да se намери информация за човек, който е записан в Blockchain мрежата, се изпълнява скрипта на функцията *queryOwnerByName* от интелигентния договор.

Интелигентните договори предоставят възможност за създаване на полици, наблюдение на тяхното състояние и чрез бизнес логиката, която може да бъде описана в тях се автоматизира процеса на обработване на застрахователни искове. Чрез интелигентни договори е възможно да се създаде застрахователна полица, да се определи застрахователният риск, да се изпълнят плащания по застрахователни искове. Блокчейнът също оптимизира процеса на презастраховане, както и операциите на брокерите. В области, където е необходим мониторинг от страна на предлагането, това ново решение ще подобри застрахователния процес.

Г.7.4. D. Todorov, H. Valchanov and V. Aleksieva, "Load Balancing model based on Machine Learning and Segment Routing in SDN", 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-4, doi: 10.1109/ICAI50593.2020.9311385.

Този доклад предлага модел, който има за цел да намали не само общото натоварване на SDN мрежата, но и да намали честотната лента и да подобри механизма за маршрутизиране в SDN мрежите. Той съчетава алгоритъм за маршрутизиране на сегменти и механизми за балансиране на натоварването, базирани на невронни мрежи. Основната цел на този модел е да изследва най-съвместимия модел на невронна мрежа за балансиране на натоварването на мрежата и да минимизира мрежовия трафик между контролера и мрежовите устройства.

В SDN има различни механизми за балансиране на натоварването, които използват два основни подхода - статично и динамично балансиране на натоварването. Разглеждат се недостатъците и проблемите на подходите и алгоритмите в подобни решения.

Моделът е разработен като крос-платформен SDN контролер, написан на езика за програмиране на C ++. Той внедрява протокола *OpenFlow* и следва специфични за операционната система системни повиквания за по-висока производителност.

Системата съдържа четири основни модула: *SDN controller module, Prediction module, Path compute module* and *Path encoding module*. Събраните мрежови параметри от системата се използват за изчисляване на оптималния път въз основа на алгоритми на невронни мрежи. Параметрите се свеждат до единичен коефициент, който след това се използва за обучение и прогнозиране.

Използвайки Q-Learning алгоритъм, процесът е разделен на два потока. Първо, няма данни за прогнозиране. За да попълни тези данни, модулът започва да се учи и получава награда за всяко успешно свързване. След като моделът е обучен, модулът може да предвиди всяка промяна на потока. След като връзката се установи, контролерът изпраща пакет за проверка на състоянието, за да получи мрежовата информация на устройството.

Когато получава информацията, контролерът я съхранява в база данни *Network Global View*. След това контролерът и суича започват да обменят ехо пакети, за да проверят връзката между тях. Тези пакети се използват за проследяване на честотната лента за връзка с устройството.

Процесът на прогнозиране следи възможните промени в натоварването на мрежата. Ако открие такива, той изпраща сигнал към *Path Compute Module*, за да актуализира *Flow* таблиците с необходимите маршрути, за да балансира натоварването на мрежата. След като оптималните пътища бъдат изчислени, те се изпращат обратно и се инсталират на суичовете. Контролерът също така уведомява процеса на прогнозиране за изпуснати мрежови устройства, което автоматично ще задейства промените в таблицата *Flow*.

Предложеният архитектурен модел комбинира алгоритми на невронни мрежи със сегментно маршрутизиране за постигане на по -добра производителност и балансиране на натоварването на мрежата. Той подобрява QoS и предоставя възможност за предсказване на претоварване на мрежовите маршрути.

Г.7.5. V. Aleksieva, H. Valchanov and A. Huliyan, "Smart Contracts based on Private and Public Blockchains for the Purpose of Insurance Services", 2020 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2020, pp. 1-4, doi: 10.1109/ICAI50593.2020.9311371.

Този доклад представя експериментално внедряване на интелигентни договори, базирани на Hyperledger Fabric Blockchain за застрахователни услуги, в сравнение с друга реализация на интелигентни договори, базирани на Ethereum Blockchain. Случаят на използване е еднакъв във всяка реализация: застрахователната компания (Org1) работи с четири компании - Org2 (broker 1), Org3 (broker 2), Org4 (broker 3), Org5 (broker 4). Всеки консорциум има двама участници - застрахователна компания и една брокерска компания. Компанията Org1 има собствен пиър Peer0, който участва в четирите консорциума и има копие от четирите смарт договора. Peer0 има основна роля в застрахователния процес, тъй като той управлява отношенията между застрахователните и брокерските компании във всеки консорциум. Предложеното решение е разработено с Metamask, Truffle и Ganache под операционната система MacOS High Sierra. Ganache създава локален блокчейн на базата на Ethereum, който може директно да изпълнява команди, както и да извършва тестове. Използва се Metamask, тъй като няма нужда да се изтегля локално копие на Blockchain. Връзката към сайта прави връзка с Ethereum. Metamask се грижи за всички заявки от и към Blockchain мрежата. Metamask може да изпълнява функция на Ethereum портфейл и да поддържа изпращане и получаване на Ethers и ERC20 токени. Truffle се използва за прилагане на интелигентния договор. Това е интегрирана система за компилиране на записаните интелигентни договори, която ги качва в мрежата на Ethereum.
Същият случай на използване в Hyperledger Fabric се основава на четири канала. Предложеният интелигентен договор, базиран на Hyperledger Fabric, е реализиран на компютъра с процесор AMD Ryzen 5 2600 6 ядра/12 нишки и с операционна система Linux Ubuntu 16.04. Освен това се използват Docker Engine версия 17.03 и Docker-Compose версия 1.8. Основната разлика от решението, основано на публичен блокчейн, където съществува мрежата, е, че в частния блокчейн първата стъпка е да се създаде блокчейн мрежата.
Предложеното публично решение с интелигентни договори за застраховка се основава на стандарта ERC20. Той е внедрен експериментално на Ethereum блокчейн. Резултатите от експериментите показват, че предложеното решение е напълно работоспособно по отношение на управлението на автоматичните плащания по одобрени искове за загуба. В предложения смарт договор бизнес логиката е по-сложна и решението е по-скъпо от решението, основано на частен блокчейн, тъй като трябва да се плати за изчислителна мощност с „ETH" токени.
Предложеното частно решение с codechains върху Hyperledger Fabric е по-гъвкаво, по-сигурно, по-бързо и по-евтино от предишното публично решение.

Г.7.6. Yuri Dimitrov, Veneta Aleksieva, Hristo Valchanov, Comparative Analysis of Prototypes for Two Touch Finger Interfaces of Smartwatch, IOP Conference Series: Materials Science and Engineering, CIEES’20, vol. 1032 (2020), pp.1-4, doi:10.1088/1757-899X/1032/1/012019, ISSN: 1757-8981, https://iopscience.iop.org/article/10.1088/1757-899X/1032/1/012019

Докладът представя сравнително проучване на предложения прототип за сензорен интерфейс за смарт часовник, активиран и управляван с два пръста, с други два прототипа.

За да се наблюдават зоните на докосване на безела, е проектиран и отпечатан специален 3D модел. Той е възможно най-близо до истинския смарт часовник според неговия размер и форма.

Първата стъпка е да се изберат размерите на 3D модела. Диаметрите на истинските интелигентни часовници варират между 34,5 мм и 58 мм, но 73% от тях са между 42 мм и 46 мм. Височината на истинските интелигентни часовници зависи от вида на функциите, но варира между 10,9 мм и 16 мм. Почти 80% от тях са между 14 мм и 15 мм. Въз основа на тази статистика избраните размери на 3D модела са - диаметър: 44 мм, височина: 15 мм, ъгъл на безела: 45^0, ширина на безела: 4 мм; цвят: бял; материал: PLA.

Втората стъпка е да се оцени в кои два отделни и обособени сектора на безела на устройството е възможно да се регистрират докосвания, за да се активира интерфейсът на устройството и да се извършат допълнителни действия с интерфейса. Подробните резултати от тази оценка са представени от авторите в други изследвания.

Третата стъпка е да се активират някои функции с този прототип на сензорен безел и да се сравни неговата функционалност с прототип с бутони. Авторите са направили това сравнение в други изследвания и основният извод е: прототипът с докосване надминава прототипа с бутони в скоростта на операциите, особено когато наборът от интерфейсни команди е по-дълъг.

Последната стъпка е да се оцени прототипът в сравнение с подобни прототипи. За да се направи сравнителен анализ на авторския прототип с други, се използват еднакви критерии за оценка. В прототипа на Oakley физическият контакт с безела на устройството е неразделна част от по-голямата част от входовете - само 17% са с два пръста. Участниците също предпочитат доминиращите си ръце и използването на палеца и показалеца си. Авторите публикуват резултатите за осем ординални посоки, но в това сравнение се използват само резултати за съвпадащите посоки с предлагания прототип. В прототипа на Yeo авторите използват няколко пръста, за да преместят целия прототип, който е с типичен размер на интелигентния часовник. Те показват, че техният прототип е конкурентен с търговските интелигентни часовници с този размер, като входните събития се генерират отзивчиво (55-61ms) и точно.

Експерименталните данни за прототипа на авторите са представени в сравнение с прототипа на Oakley и прототипа на Yeo в таблица. Според резултатите, получени за комплексната оценка, предложеният от авторите прототип е по-добър от двата други. Основното предимство на предложения прототип е неговият стандартен размер и по-малко време на докосване при дълга последователност от докосвания.

Г.7.7. Y. Dimitrov, V. Aleksieva and H. Valchanov, "Method for Body Pose Recognition based on Two-Finger Touch Bezel on Wearable Device", 2021 17th Conference on Electrical Machines, Drives and Power Systems (ELMA), 2021, pp. 1-5, doi: 10.1109/ELMA52514.2021.9503001.

Целта на представеното изследване е да предложи метод за разпознаване на позата на потребителя (легнал, седнал, изправен), когато събужда носимо устройство от режим на заспиване, и интерфейса на устройството да се активира, за да визуализира информацията и да изпълни някои команди при умишлено докосване на безела на носимо устройство с два пръста от потребителя.

Ако позата бъде успешно разпозната при активиране на интерфейса на носимо устройство, ще бъде предложен бърз достъп до функции и приложения в контекста на позата (тези, които най-вероятно ще бъдат изпълнени от потребителя). Това ще намали времето за активен режим на устройството, което ще удължи периода между две зареждания на батерията му. Разпознаването на позата на тялото може да се комбинира с други фактори, като времето през деня - например в легнало положение вечер, да се предложи бърз достъп до някои функции и приложения, а сутрин, отново в същото положение, да се предложи бърз достъп на потребителя до други функции/приложения. Друг фактор може да бъде предишна поза и/или дейност - например в изправено положение веднага след ставане, да предложи бърз достъп до някои функции/приложения, и в същата поза, но след дълъг период, да предложи други. По този начин разпознаването на пози при активиране на интерфейса на носимо устройство ще намали времето за работа с него, което ще доведе до по-дълъг период между две зареждания на батерията му. Умишлено докосване на панела за активиране на устройството с два пръста не може да бъде разпознато от друго действие и не може да възникне нежелано активиране на устройството.

Разпознаването на позата на тялото на потребителя се основава на относителната разлика в позицията на пръстите на безела при активиране на интерфейса от него в различните позиции на тялото му при използване на носимо устройство. Поради тази причина не е необходимо да се измерват ъглите в една и съща позиция за различни потребители, както и да се определят конкретни области на безела, за да се определи позицията на тялото. Достатъчно е всяко устройство / потребител да установи (след като започне да използва устройството) различните области на контакт при активиране на интерфейса и въз основа на тези различия да предвиди в каква позиция тялото на потребителя е най-вероятно в момента на активиране интерфейса.

Експерименталната група се състои от 10 души, всички с водеща дясна ръка, всички участващи доброволно в експеримента. Направени са 300 опита - по 100 за всяка позиция на тялото.

Въз основа на резултатите от експерименталните проучвания може да се предположи, че предложеният метод за определяне на позата на тялото на потребителя на носимо устройство въз основа на местоположението на пръстите на водещата му ръка върху сензорна рамка на носимо устройство, е ефективен и приложим.

Г.7.8. A. Haka, V. Aleksieva and H. Valchanov, "A Comparison Study of Decisions for Computer Network Laboratory in Distant Learning Education", 2021 17th Conference on Electrical Machines, Drives and Power Systems (ELMA), 2021, pp. 1-4, doi: 10.1109/ELMA52514.2021.9503059.

Този доклад представя сравнителен анализ на изследваните решения за дистанционно обучение по учебни дисциплини, преподаващи компютърни мрежи. Задължителната социална изолация по време на пандемия поставя нови предизвикателства пред образователната система. Необходимостта бързо да се премине към отдалечена форма на обучение наложи използването на различен образователен подход. По време на пълния lockdown бяха използвани и изследвани три подхода за обучение по дисциплини, свързани с преподаване на компютърни мрежи - симулационни продукти, реална компютърна мрежа с отдалечен достъп и виртуална компютърна мрежа с отдалечен достъп:

1) Да се използват симулационни продукти като Packet tracer, GNS3 и др.
2) В катедра „Компютърни науки и технологии“ към Технически университет- Варна е разработена от авторите реална компютърна мрежова лаборатория с отдалечен достъп. Отдалеченият достъп се осъществява чрез уеб система за управление, разработена от авторите. Citrix XenServer е избран за платформа за виртуализация, която има висока производителност, лесна поддръжка и е безплатна за използване. Основната идея на лабораторния дизайн е да се създаде snapshot на виртуалната машина (за съответната операционна система) за всеки от компютрите, като се използва възможността за snapshot на Xen.
3) За да се постигне висока гъвкавост и да се избегнат някои недостатъци на предишното решение, е внедрена експериментална виртуална инфраструктура. Базирана е на две сървърни машини Sun Fire Z20, свързани към 1G Ethernet мрежа и използващи VMware ESXi. Изборът на VMware Infrastructure 3 е продиктуван от възможностите му за многопроцесорна поддръжка, динамично балансиране и разпределение на ресурси между виртуални машини, както и мигриране на виртуални машини между отделни сървъри, без да се прекъсва тяхната работа. Въз основа на виртуалната инфраструктура бяха пуснати редица виртуални машини със съответни операционни системи. Виртуалната инфраструктура може да бъде достъпна със софтуера VMware vSphere Client.

Целта на изследването е да се оцени кое решение е най-подходящо за дистанционно обучение на студенти по дисциплини, свързани с компютърни мрежи. Разработена е система от критерии за оценка на горепосочените решения, съобразно предизвикателствата в онлайн обучението.

Сравнението се основава на предложена от авторите система от критерии, съобразена с предизвикателствата на дистанционното обучение. За да се осигури обективност при сравнението, е направена комплексна оценка на разглежданите подходи, базирана на комплексна аритметична оценка. Според резултатите от средна аритметична оценка най-подходящото решение за дистанционно обучение се определя решението с използване на виртуална мрежова инфраструктура.

Г.7.9. Veneta Aleksieva, Hristo Valchanov, Smart Contracts based on Hyperledger Fabric Blockchain for the Purpose of Health and Life Insurance Services, AIP, CIEES’21,25-27.11.2021, Rouse, Bulgaria (приета)

Този документ представя решение, основано на интелигентни договори на блокчейн, при което застрахователят плаща директно на болницата за услугите, предоставяни в полза на застрахования, и само ако застрахователната сума е недостатъчна, пациентът плаща на болницата.
Недостатъците на класическия процес в България от гледна точка на застрахователя са:
• Лицето трябва да плати директно за лечението си, което ще бъде възстановено след седмици или месеци.
• Във време, когато здравето на човека е основен приоритет, той/тя трябва да предостави документи и да посети застраховател, за да възстанови направените от него разходи, понякога многократно.
За да се избегнат тези недостатъци, решението, предложено в този доклад, е с интелигентен договор за блокчейн. Стъпките на процеса са:
1. Болест/злополука на застрахования, за която трябва да се приложи лечение.
2. Лечението включва медицински прегледи, болнично лечение, амбулаторно лечение (лекарства с рецепта, наблюдение на състоянието на застрахования от личния лекар, контролни прегледи от специалисти).
3. В случай, че лицето е задължително осигурено и/или доброволно осигурено, за заплащане на лечението, се сключва интелигентен договор, който проверява дали лицето е осигурено (ако да - нарежда покриването на сумите от НЗОК, съгласно одобрен списък със суми, които НЗОК покрива, като за останалата част от сумите за лечение проверява наличните застрахователни суми за лицето и нарежда покриването на сумите от съответния застраховател, като вписва в полицата на застрахования изразходваната сума и само в в случай че сумата на лечението не може да бъде покрита от НЗОК и застрахователя, лицето заплаща допълнително с директно плащане.
Предложената реализация се основава на Hyperledger Fabric. За всяко застрахователно дружество се създава собствен канал (консорциум). Всеки канал има своя собствена блокчейн, както и интелигентни договори (codechains), които работят само с него. Всеки консорциум има двама пиъри - Peer0 от Org1 и друг пиър от застрахователната компания. Четирите канала работят паралелно един с друг и не са видими за участниците извън тези, позволени от правилата на консорциума. Peer0 има отделни копия на четирите блокчейна. Бизнес логиката на блокчейн мрежата се реализира на езика Go.
С предложеното решение застрахователят ще избегне директни плащания. Това ще намали документите, ще премахне необходимостта от експерт за застрахователя, което ще намали оперативните му разходи и риска от едно застрахователно събитие да използва две полици с припокриване, а не с допълване. Представени са експерименталните резултати, които доказват приложимостта на предложеното решение.

Г.7.10. Veneta Aleksieva, Hristo Valchanov, Monika Vangelova, Cloud Based System for Reservation of Medical Appointments, AIP, CIEES’21,25-27.11.2021, Rouse, Bulgaria (приета)

Този доклад представя cloud система за записване на часове за клинични прегледи и консултации от разстояние. Направено е сравнение между три различни решения. Експерименталните резултати показват, че предложеното облачно решение е най-добрият вариант по отношение на скоростта на реакция, мащабируемостта, най-лесно администриране и рентабилност.
Авторите предлагат уеб-базирана система *CollosalClinic_Online*. За реализацията се използват различни инструменти като C#, HTML, CSS, JavaScript, Bootstrap, jQuery, Google API, ASP.NET. Разработката е в интегрирана среда MS Visual Studio 2017, а управлението на релационната база данни е с MS SQL Server 2019. Уеб сървърът е Apache 2.4.46, а Internet Information Services 10.0 се използва за уеб приложението и управлението на сайта, контейнеризация и бърза облачна интеграция. Тества се на локален компютър.
Втората реализация е в разпределена среда с платформа VMware Workstation Pro v.12.5.1.
Третата реализация е в облака Azure. Достъпът до приложението се осъществява чрез Интернет с URL адрес, генериран от Microsoft Azure с домейн на Azure, *https://purple-forest-09d81c203.azurestaticapps.net*. Microsoft Azure позволява да се изгради табло за мониторинг на ресурсите и производителността на системата. Формира се основно табло за управление, в което се изграждат и коригират всички необходими графики за наблюдение в реално време.
Направено е сравнение между трите реализации. Резултатите показват, че cloud-базираното решение е най-бързото, най-ефективното, има отлична производителност и устойчивост на грешки. След сравняване на това решение с пет други съществуващи решения за записване на часове за медицински прегледи и според резултатите от измерването на времето за зареждане, изтеглянето на ресурси и броя на заявките към сървърите, където се хостват приложенията, cloud реализацията на предложената система има най-добри показатели за производителност.

Г.7.11. D. Todorov, H. Valchanov, V. Aleksieva, Comparative Evaluation of Traffic Load Balancing and QoS in SDN Networks, AIP, CIEES'21,25-27.11.2021, Rouse, Bulgaria (приета)

В този доклад се предлагат различни важни критерии за прилагане на сравнителна оценка на балансирането на трафика. В края е представен комплексен сравнителен анализ на алгоритми за статично и динамично маршрутизиране за балансиране на натоварването на трафика и подобряване на QoS в SDN. За статично маршрутизиране бяха сравнени три алгоритма - алгоритъм Open Shortest Path First, shortest widest path и simple routing with link detection, предложено от авторите в други изследвания. За динамично маршрутизиране бяха сравнени три алгоритма - Extended Dijkstra's algorithm, Enhanced Interior Gateway Routing Protocol и dynamic routing with complex weights, също предложен от авторите в друго изследване.
Експерименталното проучване и резултатите са получени под Windows OS, а Mininet simulator се използва за симулиране на мрежова топология и мрежов трафик. На същата хост операционна система, на която работи контролерът, симулаторът Mininet се изпълнява като виртуална машина. За целите на експерименталното изследване, контролерът е разработен с помощта на език за програмиране C ++ и внедрява OpenFlow за управление на SDN мрежа. Контролерът поддържа основните функционалности за управление на SDN мрежа и са реализирани алгоритмите: OSPF, simple routing with link detection and dynamic routing with complex weights. Контролерът реализира всички актуални версии на комуникационния протокол OpenFlow и има модулен дизайн. Той съхранява изгледа на глобалната мрежа в оперативна памет и има възможност да инсталира правила за потока върху мрежовите ресурси, както и да обработва всеки пакет независимо, като използва входящи и изходящи пакети-съобщения. Контролерът има възможност да открие достъпността на суич с помощта на ехо съобщения, които се обменят на всеки 5 секунди. Той също така поддържа ARP съобщения за откриване на свързани хостове към мрежови ресурси и съхранява техните MAC адреси в оперативната памет, като мапва хоста към съответния суич, с който има физическа връзка.
Тестовете са направени с различни топологии за всеки алгоритъм за маршрутизиране.
Авторите предлагат система от критерии за сравнение и комплексна оценка на тези алгоритми за маршрутизиране. Ако критериите се спазват отделно, може да се види, че предложеният от авторите алгоритъм за статично маршрутизиране не дава добри резултати за „натоварване на мрежата" в сравнение с другите два алгоритма, но има равни резултати с тях за поддържане на всички мрежови топологии. Също така, спазването на критериите за механизми за динамично маршрутизиране показва, че предложеният от авторите алгоритъм има равни резултати за „Packet drop rate", „Топологии" и „Поддръжка на QoS". Поради широкия диапазон от критерии в комплексната оценка, общата геометрична и аритметична комплексна оценка на двата предложени от авторите алгоритъма е по-добра от алгоритмите, с които се сравняват.

Г.7.12. D. Todorov, H. Valchanov, **V. Aleksieva**, "Shortest path routing algorithm with dynamic composite weights in SDN networks," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 193-197, doi: 10.1109/ICAI52893.2021.9639512

В този доклад е предложен алгоритъм за най-кратък маршрут с динамични композитни тегла в SDN мрежи, използващ протокол OpenFlow. Алгоритъмът избира по-малко натоварения път въз основа на динамични тегла на node и edge, като наблюдава натоварванията на връзките между суичовете. За да открие топологията на мрежата, алгоритъмът използва LLDP за намиране на връзки между суичове и разчита на ARP съобщения за намиране на хостове, свързани с тях. По този начин той може да извършва маршрутизиране чрез призрачни суичове, което OpenFlow не поддържа.

Експерименталното проучване е направено под Windows OS, а симулаторът Mininet се използва за симулиране на топология на мрежата и трафика. Симулаторът Mininet работи на виртуална машина на същата хост машина, на която работи контролерът. Контролерът е разработен с помощта на език за програмиране C ++ и внедрява OpenFlow за управление на SDN.

Разгледаните алгоритми за маршрутизиране са:

• простият алгоритъм за маршрутизиране на авторите с откриване на връзки между хостове-източници и хостове-дестинации (от предишната ни работа, представена в доклади);

• алгоритъмът за маршрутизиране на Dijkstra, който маршрутизира трафика въз основа на минималния брой hops;

• Предложен алгоритъм за най-кратък маршрут с динамични композитни тегла.

Експерименталните резултати показват, че алгоритъмът се представя по-добре от другите 2 алгоритъма. По време на фазата на откриване на топология, той показва по-малък мрежов трафик дори с използването на LLDP. Това се дължи на огромния обмен на ARP съобщения между суичовете, използвани от алгоритъма за просто маршрутизиране за свързване на мрежови устройства.

Също така алгоритъмът постига успешно основната си цел - да се балансира натоварването на мрежовия трафик и да се осигури по-добър QoS. Той има малко увеличение на закъсненията по време на трансфер на пакети, но това се дължи на промени в потока на пакети по време на процеса на маршрутизиране, за да се предотвратят задръствания. По време на експериментите и трите алгоритма имат нулева drop rate и всички пакети се прехвърлят успешно. В допълнение, всички разгледани алгоритми за маршрутизиране успешно обработват мрежови цикли и имат ниско използване на паметта и процесорната мощност на контролера.

Г.7.13. D. Todorov, H. Valchanov and V. Aleksieva, "Simple routing algorithm with link discovery between source and destination hosts in SDN networks," 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 188-191, doi: 10.1109/ICAI52893.2021.9639742.

В този доклад е представен прост алгоритъм за маршрутизиране с откриване на връзки между хостовете- източници и хостовете-дестинации в SDN мрежи, без да се взема предвид цената на връзката. Алгоритъмът намалява съобщенията, предавани между мрежовите устройства и контролера, както и изчисляването на пътя за потоците. За внедряването и тестването е разработен контролер OpenFlow, който извършва основните взаимодействия с мрежовите устройства и използва емулатор Mininet за извършване на изследвания.
Системата съдържа два основни модула: SDN контролерен модул и Path Compute модул. Модулът SDN Controller поддържа основните комуникационни функции между контролера и сиучовете Той съхранява информация за свързаните устройства и техните таблици на потоците в базата данни Global Network View. За да се установи връзка между контролера и суича, се обменят handshake пакети. След установяване на успешна комуникация, контролерът периодично изпраща exo пакети за проследяване на достъпността на суича.
Модулът за маршрутизиране е отговорен да намери адреса на местоназначението във flow entry таблицата и да намери следващия hop за пакета на контролера. Не се взема предвид натоварването на мрежата за постигане на балансиран трафик. Модулът взема предвид първото обслужено ARP съобщение, въз основа на което взема решение къде да пренасочи пакета.
Експерименталното изследване се извършва под Windows OS. За симулиране на топология на мрежата и трафика се използва симулатор Mininet. Mininet работи на виртуална машина на хост машината. Контролерът с предложения алгоритъм за маршрутизиране работи на хоста. Контролерът е разработен с помощта на език за програмиране C ++ и внедрява OpenFlow за управление на SDN.
Експерименталните резултати показват, че алгоритъмът постига основната си цел да намали мрежовия трафик между контролера и мрежовите устройства по време на фазата на откриване. Алгоритъмът не използва Link Layer Discovery Protocol (LLDP) за намиране на връзки между мрежови устройства. По този начин елиминира допълнителния трафик и запазва мрежовата bandwidth. Алгоритъмът има нулева drop rate и всички пакети с прехвърлени успешно. Той също така показва ниски времена за прехвърляне на пакетите. Друго предимство е успешната обработка на мрежови цикли в топологията на мрежата и по-малкото използване на паметта и процесорната мощност от контролера.

Г.8. Публикации в нереферирани списания с научно рецензиране

Г.8.1. Aleksieva V., I.Zhelyazkov, Generator of Network DoS Attacks,Proceedings, pp.II-162-167, Fifth International Scientific Conference “Engineering,Technologies and Systems” TECHSYS 2016, 26-28 May 2016, Plovdiv, ISSN 2367-8577

Този доклад представя система за генериране на мрежови DoS атаки, използваща протоколи от TCP / IP протоколното семейство - UDP, TCP и ICMP. Целта на разработената система е за образование и предлага универсални инструменти за симулиране на различни видове атаки. Реализирани са DoS атаки с различни параметри.

За реализиране на предложения генератор на DoS атаки е избрана операционна система - Kali Linux 2.0 sana, тъй като е оптимизирана за извършване на тестове за проникване и много от ограниченията, наложени от други популярни дистрибуции на Linux и в повечето версии на Windows (с изключение на Windows XP/2000/Server 2000/2008), по отношение на RAW socket, отсъстват. Избраната среда за програмиране е Code Blocks 10.05, с компилатора GNU GCC.

За да се предотвратят възможни злоупотреби с този предложен не-комерсиален генератор, се прилагат много ограничения като:

• Забрана за многократно инсталиране на софтуера - стартирането му в паралелни процеси;

• Ограничен е максималния брой едновременно работещи нишки до 500. Всеки tread след 500 ще изчака във FIFO опашката да бъде стартиран;

• Броят на реализациите на различни видове атаки се намалява до четири най - популярни атаки - наводнение с UDP пакети, наводнение с TCP пакети, наводнение с ICMP пакети (има две реализации - Ping of Death и broadcast атаки), наводнение с TCP SYN съобщения;

• Максималният общ брой байтове, изпратени на "жертвата", е ограничен до максимална стойност от тип unsigned long, независимо от продължителността на атаката;

• Максималният размер на отделни ICMP пакети е 64 байта;

• Буферът за данни на UDP и TCP пакети е ограничен до 27 байта.

Предлаганият генератор на DoS атаки предоставя следните функции:

• набор от популярни DoS атаки за извършване на симулационни тестове;

• набор от инструменти за персонализиране на параметрите на атаката;

• инструменти за автоматизирани тестове с цел повторно симулиране на различни сценарии с минимална намеса на потребителя;

• добро представяне и високо ниво на контрол върху извършените тестове;

• ниски системни изисквания;

• най -простият и интуитивен набор от команди;

• създаване на лог файлове за анализ.

Представени са резултатите от тестовете за всеки вид мрежови атаки (UDP/ TCP flood attack, ICMP flood attack, SYN flood attack). Тестовете се проведени в две подобни експериментални ситуации - атакуваната машина в първата ситуация работи под Linux Slackware, а във втората - под Windows 7. Тестовете са проведени в локална Ethernet мрежа.

Г.8.2. Хъкъ А., В. Алексиева, Моделиране на разпределяне на честотната лента в пасивни оптични мрежи //Компютърни науки и технологии, ТУ-Варна, 2016, бр.1, с.45-51, ISSN 1312-3335.

В този доклад се предлага софтуерна симулация за анализ на ефективността на разпределяне на честотната лента в пасивни оптични мрежи. Представен е алгоритъм за разпределение на ресурсите в два етапа за максимално усвояване на честотната лента чрез използване на ортогонално честотно мултиплексиране за пасивни оптични мрежи (OFDM-PON) - първо се разпределя времевия интервал (таймслот) за всяко абонатно устройство (Optical Network Unit -ONU) и второ се подреждат подканалите, състоящи се от група подносещи честоти. Прилагането на предложения подход, базиран на динамично разпределение на подносещите канали, осигурява ефективно разпределяне на честотната лента и намалява закъсненията при предаване на заявките на отделните потребители.

PON мрежата се състои от централизиран Optical Line Termination (OLT) от страната на Интернет доставчика и множество Optical Network Unit (ONU) устройства от страната на потребителите. ONU-тата споделят ресурси в общ оптичен поток, свързващ ги с OLT.

PON системата трябва да приложи подходящ MAC механизъм, за да се осигури ефективно предаване, да се използват ефективно мрежовите ресурси, да се арбитрира достъпа до споделената среда и да се избегнат колизии на данни.

В настоящата разработка е представен алгоритъм за разпределение на ресурсите в два етапа за максимално усвояване на капацитета на връзката чрез използване на OFDM-PON, т.к. при OFDM-PON се използва синхронна структура на фрейма, за да се осигури диференциалното обслужване на заявките. При разпределяне на ресурсите предложеният алгоритъм първо разпределя времевия интервал (таймслот) за всяко ONU и след това подрежда подканалите (група от подносещи честоти). Този алгоритъм трябва да отговаря на две ограничения:

- изчисленията за разпределението на ресурсите се правят за единичен фрейм;
- едно ONU използва само един подканал, за да изпрати към OLT данни за множество услуги в рамките на продължителността на кадъра.

Предложеният алгоритъм се прилага само в посока upstream и се изпълнява в две фази:

1) Разпределение на времевия интервал (таймслот) - назначава временно подканал за всяко ONU

2) Преразпределение на подканалите - временният подканал j за ONU [i, j] ще бъде заменен с потвърден подканал, в който има достатъчно ресурс за разполагане на ONU[i+1, j], като по този начин се минимизира броят на отложените за следващ фрейм ресурсни блокове, и се уплътнява честотната лента, т.е. не остават свободни подносещи.

За анализиране на предлагания в настоящото изследване алгоритъм за разпределяне на честотната лента се създава модел на трафика за няколко OLT, но визуализация на матрицата за предаване се извежда само за OLT по избор.

Създадена е база данни за съхранение на данните от отделните експерименти за отделните OLT и за свързаните към тях потребители.

Г.8.3. В. Алексиева, Симулационна среда за реализация на приоритетно базирана Zigbee мрежа, John Atanasoff Society of Automatics and Informatics, Sofia, October 4-7, 2016, ISSN 1313-1869, с.125-128

В доклада е предложен модифициран алгоритъм за изграждане на приоритетно базирана и енерго-балансирана Zigbee мрежа. Модифицираният алгоритъм определя приоритетите на устройствата чрез метода на ценообразуването, където приоритетът на крайните устройства и енергийното ниво на рутерите се явяват като цена, която са готови да заплатят. На тази база се изгражда ефективна енерго-балансирана приоритизирана дървовидна структура от Zigbee устройства.
При този метод се приема, че рутерите служат само за изграждане на топологията и не функционират като крайни устройства. Всяко устройство (крайно устройство или рутер) разполага с поле payment (разплащателна способност), което се явява приоритет за крайните устройства и енергийно ниво за рутерите. Координаторът заедно с рутерите притежават и поле за цена (charging rate), която трябва да се заплати, за да се свържат към тях. Следователно колкото по-голяма е разплащателната способност на крайното устройство, толкова по-висок приоритет има то. При рутерите колкото по-висока е стойността на разплащателната способност, толкова повече енергия имат, следователно трябва да стоят на по-ниско ниво в дървото, за да могат да обслужват повече устройства.
Когато крайно устройство има по-голяма разплащателна способност от цената на кандидат-родителя му, то се свързва към него, променяйки цената му. В този модифициран алгоритъм първи се свързват рутерите, за да могат да изградят мрежата, след което към тях се свързват крайните устройства. При свързване на рутер към рутер или на рутер към координатора, цената на родителя не се променя. В случая, при който остане устройство с недостатъчна разплащателна способност, то се свързва към рутера с най-малък брой деца.
Създадена е симулационна среда за реализация на предложения алгоритъм, която позволява визуализация на Beacon-Only-Period метода на предаване между устройствата при Zigbee дървовидна топология на мрежата. Създадена е база данни за съхранение на данните от отделните експерименти за координаторите и за свързаните към тях устройства. С цел универсалност на създадения симулатор и поради факта, че няма единно утвърден превод на терминологията, свързана със ZigBee, за реализация на симулатора е избран английски език. Чрез времедиаграма се визуализира предаването на пакети по Beacon-Only-Period метода за избягване на директни колизии. Настоящият симулатор предлага възможност за изграждане на всяка реална топология, която се състои и от крайни устройства.
Направен е сравнителен анализ на средната скорост на предаване на пакетите за различна продължителност на предаване през Zigbee мрежа, създадена по класическия метод и по метода на ценообразуването. Наблюдава се подобрение на средната скорост в Zigbee топология, изградена по втория метод.

Г.8.4. З. Митев, С. Вълчанова, В. Алексиева, Персонализирано наблюдение и управление на виртуални инфраструктури на база Zabbix, Session Schedule&Abstracts, 55th Annual Science Conference of Ruse University, Smart Specialization-innovative Strategy for Regional Economic Trransformation, Русе, 28-29.10.2016, University of Ruse Publishing Center, с.163, ISSN 1311-3321

Това е резюме на наградения доклад Г8.7 с „Best paper” в юбилейна книжка на РУ:

В този доклад се предлагат инструменти за мониторинг и управление на виртуални инфраструктури, базирани на Zabbix- мониторинг на уебсайтове, попълване на информация за хоста, мониторинг на процесите в услугите на Windows, изпращане на известия до клиенти на Gmail, мониторинг на Apache сървър, мониторинг на размера на кошчето и наблюдение в реално време на допълнителни устройства, свързани към даден хост и т.н.

Резултатите показват, че тези инструменти са напълно подходящи за голяма виртуална инфраструктура с критични устройства. Тази платформа напълно осигурява постоянен мониторинг, своевременно уведомяване на всички отговорни потребители, когато възникне проблем и преодолява проблема с помощта на скриптове на външен потребител.

Г.8.5. В.Алексиева, И.Желязков, Изследване на DoS атаки, UNITECH’16,18-19 November 2016, GABROVO – vol. II, стр,162-167, ISSN 1313-230X

Този доклад представя изследване на мрежови DoS атаки, използвайки протоколи от TCP / IP протоколното семейство - UDP, TCP и ICMP. Изследването е направено в лабораторна мрежа, използваща разработена от авторите в предходно изследване система за генериране на DoS атаки. Целта на изследването с разработената система е да предложи универсални инструменти за симулиране на различни видове атаки и за измерване на вредата от тях. Реализирани са DoS атаки с различни параметри.
Тестовете са проведени в локална Ethernet или WiFi мрежа:
1. Тест за натовареност в Ethernet мрежа при DoS атака
Целта е да се проследи състоянието на системата на атакуваната машина по време на провеждане на продължителна DoS атака. При първите тестове параметрите на атакуваната машина са: CPU Intel Core2Duo T7700 2x2.40 GHz; RAM(physical) 2.00GB ddr2 ; OS Slackware 32-bit. Параметрите на атакуващата машина са: CPU Intel Core i7 vPro 4x2.13 GHz;RAM(physical) 4.00GB ddr3; OS Kali Linux 2.0 sana 64-bit. Проведеният тест е само с продължителна ICMP атака към атакуваната машина. Атакуващата машина стартира 100 нишки, симулирайки атака от 100 различни източника. В резултат от атаката, натоварването на процесора на атакуваната машина нараства с над 50%. Аналогично са проведени и други атаки. При първите тестове се наблюдава драстичен скок в натоварването на процесора след старт на ICMP атака, както и при изпълнение на другите видове атака. Изключение прави SYN flood атаката, която генерира голям обем входящ трафик към атакуваната машина. В резултат от ICMP атаката, атакуваната машина не успява да отреагира навреме на различните действия на потребителя.
Целта на втората група тестове е да бъде атакувана по-мощна машина от предходата и да се наблюдава ефекта върху системата по време на всяка една атака в Ethernet среда. Параметрите на атакуваната машина са: Windows 10 Pro; CPU Intel Core i5 430M 4x2.27 (4 logical cores); RAM(physical) 4.00GB ddr2. Параметрите на атакуваща машина са: Kali Linux 2.0 sana 64-bit, CPU Intel Core i7 vPro 4x2.13 GHz, RAM(physical) 4.00GB ddr3. При вторите тестовете за натоварване, където бива атакувана машина с четириядрен процесор, за всяка атака се изпълняват паралелно 500 нишки (т.е. реализира 500 отделни атаки). Натоварването, на което е подложена атакуваната машина е значително по-малко (с до 30% по-малко) от наблюдаваното натоварване при първата група тестове.
2. Тест за натовареност в WiFi мрежа при DoS атака
Целта на тази група тестове е да се проследи ефекта върху системата на атакуваната машина по време на всяка една атака в WiFi мрежа. Параметрите на атакуваната машина са като в предходните тестове.
Поради по-голямата пропускателна способност на медния кабел за едно и също време входящия трафик към атакуваната машина е значително по-малък от този, пристигащ при пренос на данните по безжична мрежа, което се отразява и на натоварването на процесора. По малкият обем данни не принуждава операционната система на атакуваната машина да използва в намален капацитет процесора.

Г.8.6. V.Aleksieva, H.Valchanov, M.Magdziak-Toklowicz, R.Wrobel, R.Wlostowski, Transmission of vibrations from the engine to the car body, Journal of KONES Powertrain and Transport,vol.23,No.4 2016, pp.17-23, ISSN:1231-4005

Вибрациите се превърнаха във важен фактор за превозните средства. Вибрационните тестове помагат да се идентифицира и след това да се настрои автомобилното превозно средство, за да се подобри здравината на конструкцията. Вибрационното изпитване често се извършва с помощта на лазерна доплерова виброметрия (LDV) - устройство, което се използва за безконтактно измерване на вибрациите на повърхността. Лазерният лъч се насочва от устройството към повърхността, която представлява интерес, а амплитудата и честотата на вибрациите се извличат от честотата на доплеровото изместване на отразения лазерен лъч поради движение на повърхността. Високите стойности на вибрации, предавани от двигателя, и начина, по който влияят значително върху каросерията на превозното средство и водача са изследвани.

Статията представя резултатите от изследванията, проведени върху превозни средства, задвижвани от три различни двигателя и обороти. Изпитанията бяха проведени на динамометър на двигателя при еднакви условия на околната среда. Два от двигателите бяха с искрово запалване, включително един с двигател с компресор и двигател със запалване под налягане.

Измерванията са направени с помощта на лазерна доплерова виброметрия, използваща бърза трансформация на Фурие. Полученият спектър се използва за по-нататъшен анализ за определяне на нивото на ускорение при различни честоти. Получените показания за бързо преобразуване на Фурие са използвани за начертаване на графики на честотното ускорение.

С увеличаването на скоростта на въртене на коляновия вал (и намаляване на продължителността на периода) се появяват допълнителни колебания при всички видове превозни средства (те се виждат ясно дори при най -ниската скорост на двигателя с компресор), но вибрационният сигнал е със стационарен характер.

Диаграмите показват недвусмислено, че амплитудата на вибрацията, независимо от целта на измерване, е най-голяма за превозното средство с двигател със запалване под налягане и най-ниска за превозното средство с двигател с искрово запалване (без налягане). В същото време колебанията и средните стойности на сигналите показват, че превозното средство с дизелов двигател е най - ергономично, докато превозното средство с двигател с искрово запалване със свръхкомпресор е най -малко ергономично.

Г.8.7. З. Митев, С. Вълчанова, В. Алексиева, Персонализирано наблюдение и управление на виртуални инфраструктури на база Zabbix, Best Paper, 55th Science Conference of Ruse University, Русе, 28-29.10.2016, University of Ruse Publishing Center, с229-234, ISSN 1311-3321

В доклада е предложено решение, реализиращо няколко скрипта за пълноценно и качествено следена на виртуални инфраструктури - за мониторинг на уеб сайтове, попълване на информация за хоста (клиента), следене на процеси в Windows services, изпращане на нотификации към Gmail клиенти, мониторинг на Apache сървър, следене големината на Recycle bin-а в реално време, следене на допълнително закачени устройства към даден хост.

Zabbix може да използва правило за търсене на ниско ниво, за да открие автоматично VMware хипервайзори и виртуални машини. Наборът от данни по подразбиране в Zabbix предлага няколко готови за използване шаблони за мониторинг на VMware vCenter и vSphere. Тези шаблони съдържат предварително конфигурирани правила, както и редица вградени проверки за мониторинг на виртуални инсталации. В допълнение към вградените проверки в Zabbix е възможно да бъдат създадени и персонализирани проверки. Zabbix агентът притежава и способността да изпълнява потребителски скриптове. Така функционалността му може да бъде увеличена според персоналните потребности на съответната виртуална инфраструктура чрез създаване на скриптове, написани на Shell script, Perl, Python, Ruby и т.н.

За тестова реализация на системата са използвани Linux сървър с дистрибуция OpenSuse v.13.1 и тестова машина с Windows Server 2008. И двете машини са виртуални и работят върху VMWare ESX сървър. На Linux сървъра са инсталирани Zabbix server, Zabbix agent, Zabbix frontend, Postfix mail server, MySQL database, Apache server, SNMP server, Уеб браузър без графичен интерфейс и текстов редактор. На Windows Server 2008 е инсталиран SNMP сървър и е конфигурирана възможността Zabbix агента да изпраща съобщения към адреса на Zabbix сървъра.

За целите на експерименталните изследвания за да се реализира наблюдение и управление на виртуална структура с критични компоненти, са разработени следните скриптове:

1. Автоматично въвеждане на информация за хоста в Zabbix frontend-а
2. Следене на процеси, като ping до хост, ниво на използване на процесора, работа на Apache сървъра и нотификации
3. Следене работата на процесите в Windows Services
4. Мониторинг на уеб сайт в реално време
5. Водене на одит лог

Получените резултати доказват, че за големи инфраструктури с критични устройства е най-подходяща употребата на Zabbix. Тази платформа категорично гарантира постоянен мониторинг, навременно уведомяване на всички отговорни потребители при възникване на проблем, както и неговото отстраняване, чрез използване на външни потребителски скриптове.

Г.8.8. V.Aleksieva, Simulation Framework for Realization of Priority-based ZigBee Network, // Information technologies and control, Sofia, vol.14, issue 2, 2016, ISSN 1312-2622, pp.20-27, https://www.degruyter.com/view/j/itc.2016.14.issue-2/itc-2017-0003/itc-2017-0003.xml, DOI: https://doi.org/10.1515/itc-2017-0003, Print ISSN: 1312-2622; Online ISSN: 2367-5357

ZigBee е безжична технология, която осигурява ниска консумация на енергия на устройства в WPAN за приложения, предаващи данни с ниска скорост, които изискват дълъг живот на батерията и сигурна мрежа. ZigBee дава ефективни начини за поддържане на QoS (качество на услугата), функционалност и управляемост, тъй като устройствата ZigBee могат да предават данни на големи разстояния (повече от 100 метра), като предават данни през мрежа от междинни устройства, за да достигнат до по –отдалечени устройства.

В тази статия е предложен симулатор за технологията ZigBee. Той внедрява модифициран алгоритъм за изграждане на приоритетна и енергийно балансирана WPAN мрежа и визуализира начина на предаване.

Един подход за решаване на проблема с директни колизии е Time-Division подходът. Друг подход е Beacon-Only Period. Предложението за решаване на проблема с индиректни колизии е Reactive метод. В този метод всяко устройство (маршрутизатор или крайно устройство) трябва да има способността да предава информация за времето за beacon frames от своя родител до своите съседи. Този подход е сложен за сортиране на таблица от съседните координатори, тъй като те се нуждаят от чести актуализации, но елиминира възможността за развитие на непреки колизии.

Настоящият подход предлага модификация на алгоритъма, предложен в предишни авторски изследвания. В основата на предложения алгоритъм стои метод на ценообразуване, въз основа на който се изгражда ефективна енергийно балансирана приоритетна дървовидна структура на устройствата ZigBee.

В този метод се приема, че рутерите служат само за изграждане на топологията и не работят като крайни устройства.

В този модифициран алгоритъм първо се свързват рутерите в дървото на топологията, за да може да се изгради мрежа, след което крайните устройства се свързват с тях. Когато се свързват рутер към рутер или рутер към координатор, цената на родителя не се променя. В случай, че устройството е с достатъчна текуща платежна способност, то се свързва към рутера, който има най-малък брой деца.

Този алгоритъм променя топологията, получена без приоритети към по-добра топология, където устройствата работят с ниска консумация на енергия.

Дадени са резултатите от проведените експерименти. Симулаторът, създаден от автора в друго изследване се използва за целта. За да се направи извод за броя на възникналите колизии, се следи средната скорост на предаване на пакети с различна дължина на предаване чрез мрежата ZigBee, създадена по класическия метод и метода на ценообразуване. И в двата случая мрежата ZigBee се състои от едни и същи устройства със един и същ обем предавани данни. Налице е подобрение в средната скорост на предаване в топологията на мрежата, постигната с предложения алгоритъм за ценообразуване.

Г.8.9. Aleksieva V., I. Zhelyazkov, Generator of Network DoS Attacks, Proceedings//Journal of the technical University of Sofia Plovdiv Branch, Bulgaria, Fundamental science and Applications, vol.22 ,2016, pp. II-101-106, Plovdiv, ISSN 1310-8271

Тази статия представя разширена и допълнена версия на Г8.1, където е представена система за генериране на мрежови DoS атаки, използваща протоколи от TCP / IP протоколното семейство - UDP, TCP и ICMP. Целта на разработената система е за образование и предлага разнообразни инструменти за симулиране на различни видове атаки. Реализирани са DoS атаки с различни параметри.
За реализиране на предложения генератор на DoS атаки е избрана операционна система - Kali Linux 2.0 sana, тъй като е оптимизирана за извършване на тестове за проникване и много от ограниченията, наложени от други популярни дистрибуции на Linux и в повечето версии на Windows (с изключение на Windows XP / 2000 / Server 2000/2008), по отношение на RAW сокети, отсъстват. Избраната среда за програмиране е Code Blocks 10.05, с компилатора GNU GCC.
Предлаганият генератор на DoS атаки предоставя следните функции:
• набор от популярни DoS атаки за извършване на симулационни тестове;
• набор от инструменти за персонализиране на параметрите на атаката;
• инструменти за автоматизирани тестове с цел повторно симулиране на различни сценарии с минимална намеса на потребителя;
• добро представяне и високо ниво на контрол върху извършените тестове;
• ниски системни изисквания;
• прост и интуитивен набор от команди;
• създаване на лог файлове за анализ.
Представени са резултатите от тестовете за всеки вид мрежови атаки (UDP/ TCP наводнение, ICMP наводнение, SYN наводнение). Тестовете се предоставят в две подобни експериментални ситуации - атакуваната машина в първата ситуация работи под Linux Slackware, а във втората - под Windows 7. Тестовете се предоставят в локална Ethernet мрежа.

Г.8.10. Aleksieva V., A. Haka, Simulation framework for realization of priority-based LTE Scheduler, Techsys 2017, Technical University of Sofia, brunch Plovdiv, pp. II-181-185, ISSN Online: 2535-0048

В този доклад е предложен симулатор за LTE технология, който реализира алгоритъм, базиран на приоритети за LTE Scheduler, който пренарежда пакети, въз основа на механизъм за класификация.
Целта на предложения алгоритъм е да се постигне запазване възможно най-висока мрежова пропускателна способност на малка цена само с малко повече предавания. Функциите за управление на QoS в мрежите за достъп са отговорни за ефективното разпределение на ресурсите на безжичния интерфейс. Те обикновено се определят като алгоритми за управление на радиоресурси и включват управление на захранването, контрол на връзката за прехвърляне, контрол на достъпа, контрол на натоварването и пакети за управление, но пряко свързани с QoS на ниво клетка са последните три. Те се използват за осигуряване на максимална производителност за отделни услуги.
Настоящият документ предлага алгоритъм за обслужване на UE при разпределение на ресурси в uplink на LTE мрежата, съставен от два модула - чрез механизъм за контрол на допускане (admission control) и планировчик (Scheduler). Според натоварването на мрежата, контролът за допускане за приемане на заявки управлява броя UE, които могат да влязат в Планировчика, за да се избегне претоварване на системата с твърде много UE.
Планировчикът разпределя RBs между UEs според нуждите на UEs по приоритети.
Създадена е симулационна среда за внедряване и проучване на предложения алгоритъм. Използваният софтуерен инструмент е Visual Basic 2010. На този етап на разработка на симулатора данните от различни експерименти се изпращат във формат .xls за последваща оценка.
Резултатите дават основание да се заключи, че представеният алгоритъм за контрол на допускането в Scheduler за LTE мрежата може да се приложи успешно при брой на UE под 100, тъй като независимо от интензивността на заявките на активните UEs средното време за връзка е под 25ms - време, напълно отговарящо на изискванията на стандарта 3GPP.
Резултатите от симулацията показват, че предложеният механизъм подобрява QoS, но наблюдаваните параметри се влошават, когато обслужването на повече абонати е свързано с планиране с приоритет, при което може да не се обслужват по-малко приоритетните опашки в случай на претоварване или претоварване на мрежата. Представени са drop ratio с приоритизация и без приоритизация. При този алгоритъм винаги е осигурено минимално предаване за всички класове услуги с различни характеристики, според приоритета.

Г.8.11. Aleksieva V., D. Dinev, Simulation framework for realization of quality of services in LiFi network, John Atanasoff Society of Automatics and Informatics, Sofia, October 4-6, 2017, ISSN 1313-1869, с.201-204

В доклада е предложен алгоритъм за разпределяне на ресурса в LiFi мрежа на закрито, който определя приоритетите на устройствата и разпределя ресурсните блокове в един времеви слот между тях на база на този приоритет. Създадена е симулационна среда за неговата реализация, която позволява визуализация на метода на предаване между устройствата при LiFi инфраструктурна топология на мрежата "Звезда" с двупосочна комуникация, в която ресурса се поделя между потребители в uplink посока на база на оригинален алгоритъм за тяхната приоритизация.

Чрез предложения алгоритъм се разпределят ресурсните блокове в един времеви слот като се приоритизира трафика по няколко параметъра:

1. Първият критерий е разстояние до точката за достъп, което е ограничено според радиуса на обхват на всяка точка за достъп. По-близкото устройство е с по-висок приоритет. При равно разстояние се преминава към следващия критерий.
2. Вторият критерий е дали устройството е мобилно или статично. Ако то е мобилно трябва да се въведе скорост, с която то се движи. Симулацията е за LiFi система на закрито, затова то не може да се движи с повече от 5км/ч (средна скорост на движение на човек). По-приоритетни са мобилните устройства пред стационарните, но устройството, което е с по-ниска скорост е с по-висок приоритет.
3. Третият критерий са типовете на услугите. Всяка точка за достъп може да предоставя на един потребител един или повече типове услуги. Всяка една от тези услуги спада към съответен клас, който има различен приоритет според QoS параметрите. Handover Calls, Link Recovery Calls и Voice Calls спадат към класа, който е с най-висок приоритет (Class1). Video Calls спада към Class2, който е следващ по приоритизиране. Browsing, HDTVи Voice Messeges са към Class 3, а служебният трафик (Background traffic) спада към най-ниско приоритетния клас – Class4.

LiFi е нова за пазара технология, изключително скъпа в сравнение с алтернативни решения и с малък брой комерсиални реализации. Към момента липсват симулационни среди, с които да се изследват параметри на LiFi технологията, свързани с подобряване на QoS. Това именно налага разработването на собствени решения за изследване и тестване на подходи за решаване на възникващите проблеми при възможни реализации на LiFi. За реализиране и изследване на предлагания в настоящото изследване алгоритъм е създадена симулационна среда. Използваното програмно средство е Visual Basic 2010. Създадена е база данни за съхранение на данните от отделните експерименти за точките за достъп и за свързаните към тях устройства. С цел универсалност на създадения симулатор и поради факта, че няма единно утвърден превод на терминологията, свързана с LiFi, за реализация на симулатора е избран английски език.

Г.8.12. Aleksieva V., Haka A., Simulation framework for realization of priority-based LTE Scheduler//Journal of the technical University of Sofia Plovdiv Branch, Bulgaria, Fundamental science and Applications, vol.23 ,2017, pp. II-101-106, Plovdiv, ISSN 1310-8271

Тази статия е разширена и допълнена версия на доклада Г8.10. В тази статия е предложена симулационна среда за LTE технология, която реализира алгоритъм, базиран на приоритети за LTE Scheduler, който пренарежда пакетите, въз основа на механизъм за класификация.
LTE използва технология за многократен достъп (OFDMA), където общата честотна лента е разделена на ресурсни блокове (RB) в честотната област. Данните се предават в транспортни блокове (TB) в един интервал от време за предаване (TTI) за 1 ms. Всеки RB се състои от 12 подносещи (всяка от тях е 15 kHz). Фреймът е 10ms и е разделен на 10 равни подфреймове. Всеки подфрейм съдържа 2 слота*0.5ms. Всеки RB е свързан с един слот във времето. Един TB е свързан с 1 подфрейм и това е минималната единица за планиране. Правилото за обслужване е да се намери първо място, което да побере TB. Ако в текущия TTI няма достатъчно RB, планировчикът се опитва да намери ресурси в следващия TTI. Тази стратегия минимизира латентността на отговора, което е най -добрата практика за чувствителен към забавяне трафик. Но тази процедура не е приложима за предаване на beacons (които се изпращат между устройствата на всеки 100 ms), поради спешността на информацията, която се предава, поради което съществуват резервирани ресурсни блокове за поемане на временно претоварване. Настоящата статия предлага алгоритъм за обслужване на UE за разпределение на ресурси в uplink връзка на LTE мрежата, съставен от два модула - механизъм за контрол на допускане (admission control) и Scheduler. Според натоварването на мрежата, контролът за допускане за приемане на заявки управлява броя UE, които могат да влязат в Планировчика, за да се избегне претоварване на системата с твърде много UE. Планировчикът разпределя RBs между UEs според нуждите на UEs. Разпределението на ресурсите в Планировчика се основава на приоритета на трафика (най -високият е първият):

1. Video, voice, interactive gaming – default bearer, non-GBR
2. E-mail, chat, ftp, www, p2p, file sharing – default bearer, non-GBR
3. Video streaming- GBR
4. Video call- GBR
5. Online gaming- GBR
6. VoIP call- GBR
7. IMS Streaming– default bearer, non-GBR
8. Speed of UE
9. Distance to eNodeB
10. Payed priority

Създадена е симулационна среда за внедряване и проучване на предложения алгоритъм. Тя има модулна архитектура. Въвеждането на данни за всяко устройство започва от първоначалните параметри за eNodeB.

Г.8.13. Алексиева В., Ж.Димитров, Тестване на уязвимости в сигурността при безжични мрежи, UNITECH’17,17-18 November 2017, GABROVO, vol.II, pp. 209-213, ISSN 1313-230X

Този доклад представя инструменти за тестване на уязвимости в безжичните мрежи, базирани на техниките " man-in-the-middle" и social engineering. Работи под Kali Linux с многоезичен интерфейс. Инструментът дава възможност за проверка на нивото на защита с парола за WiFi мрежи с различно криптиране, като WEP, WPA и WPA2. Разработката е модулна и позволява лесно разширяване. Представени са резултатите от експериментални изследвания.

Настоящата разработка използва активния метод за изследване на сигурност на безжични мрежи и представя средство за изследване на уязвимости, разработено под Kali Linux. Проведените и представени тук тестове на безжични мрежи са за учебни цели и са направени в лабораторни условия.

За реализация на генератора на атаки е избрана операционна система - Kali Linux 2.0 sana, т.к. тя е оптимизирана за извършване на penetration тестове и редица от рестрикциите наложени в други популярни Linux дистрибуции и в повечето версии на Windows (с изключение на Windows XP/2000/Server 2000/2008), по отношение на RAW сокетите, отсъстват. Kali Linux вече е официално достъпен и за смартфони като Nexus 5, Nexus 6, Nexus 7, Nexus 9, Nexus 10, OnePlus One, и някои модели на Samsung Galaxy, което прави възможно инсталиране на приложението на мобилно устройство.

Необходимите модули за правилната работа на приложението са: Aircrack-ng, Aireplay-ng, Airmon-ng, Airodump-ng, Awk, Curl, Macchanger, Mdk3, Nmap, Pyrit и др. Ако някое от тях не е инсталирано, приложението дава нотификация за необходимата инсталация и спира работа.

С представеното приложение за тестване на устойчивостта на безжични мрежи са атакувани безжичните рутери за извличане на паролите им. Извършени са няколко типа атаки, като при всяка е измервано времето, за което се постига пълен достъп до атакуваната безжична мрежа.

С предложеното решение може да се помогне за усъвършенстване и тестване на защитата на всяка една безжична мрежа, но и да се даде възможност за извършването на тестове и симулации в реално време, максимално доближаващи се до реалните условия, при които мрежата ще функционира в критични за нейната сигурност моменти.

В настоящият доклад са представени и резултати от експерименти, които доказват ефективността на предложеното софтуерно средство за изследване уязвимостта в сигурността при безжични мрежи. Неговата модулна реализация позволява в бъдеще да се имплементират и други видове популярни атаки, които не са насочени само към безжичните мрежи.

Г.8.14. Aleksieva V., S. Slavov, Managed active directory in directory–as-a-service, Techsys 2018, Technical University of Sofia, brunch Plovdiv, pp. II-145-II-150, ISSN Online: 2535-0048

В този доклад е предложена уеб-базирана система за управление на AD, която осигурява безпроблемно и просто изживяване на IT администраторите и синхронизира директории между локални и cloud, като по този начин една и съща идентичност се използва и в двете среди.
Разработената уеб-базирана система (MATEX) управлява AD. Сървърната страна се основава на скриптове и командлети на PowerShell. Системата е разработена с Visual Studio 2010, ASP.NET, C#и Windows Powershell.
MATEX работи на три виртуални машини (VM) - два сървъра (BGVARNADC01, JPTOKYODC01) и един клиент USTESTPC01. На първия сървър BGVARNADC01 (Windows Server 2012R2 Std) / VM са стартирани AD Primary Domain Controller (PDC) и всички притежатели на роли на FSMO, DHCP Primary server, ISS Web server, File server, SMTP server, Backup server. На втория сървър JPTOKYODC01 (Windows Server 2012R2 Std)/ VM са стартирани сървър за AD Domain Controller, DHCP сървър за архивиране, WSUS сървър, файлов сървър, резервен сървър. Третата VM USTESTPC01 (Windows 7 Pro)/VM има роля на клиентска работна станция и там са конфигурирани Dynamic DNS запис за присъединяване към IP настройките на домейна от DHCP сървъра.
Домейнът Matex.com се състои от два контролера на домейни (DCs) - BGVARNADC01 и JPTOKYODC01, които двупосочно възпроизвеждат всички AD контейнери и DNS контейнери. По този начин промяната или действието, направено на един DC, се репликира и е видимо за другия. Времето за репликация по подразбиране е един час.
Структурата на организационната единица (OU) е разделена на 3 нива за по - лесно управление и класификация на потребителите и ресурсите (регионално ниво - Африка, Азия, Европа ...; ниво на страната - Китай, Индия, Япония ...; ниво на сайта - Фуджи , Кобе, Токио ....). Функционалността на DNS в MATEX е интегрирана в Active Directory като динамично регистриране, разрешено само за клиенти на домейна. Този факт не позволява регистрирането на персонални компютри извън домейна. Функцията Aging / Scavenging е зададена и за двете опции на 7 дни. Това означава, че динамичният DNS запис ще бъде автоматично изтрит след 14 дни, ако клиентската машина е неактивна през това време.
За да се определи ефективността на MATEX се прилагат различни тестове, чрез симулиране на възможност за работа за определен брой потребители, които използват сайта едновременно. MATEX управлява едновременно заявки на 5, 10 и 15 потребители едновременно. В случай на 20 едновременно активни потребители, има наблюдавани моменти, в които производителността спада значително в определени моменти.
Средното време за множество "кликвания" е измерено за различен брой потребители (5,10,15), направени едновременно. То е много малко. За 20 потребители средното време се удвоява. Изводът е, че 20 е границата на едновременно активни потребители, които използват MATEX, защото над този брой производителността и продуктивността се забавят.

Г.8.15. Dimitrov Y., V. Aleksieva, Two-finger Touch on Wearable Device Bezel Method for User Pose Recognition, Proceeedings of the 1st International Conference “Applied Computer Technologies” ACT2018, 21-23 June 2018, Ohrid, Macedonia, UIST”St.Paul the Apostle”, pp. 11-14, ISBN987-608-66225-0-3

Този доклад представя изследване дали има връзка между позата на потребителя (изправен, седнал или легнал) и позицията на докосвания с два пръста върху рамката на устройството за носене, причинени от разликата в стойката на ръцете на потребителя. Намирането и доказването на такава връзка ще отвори много възможности за подобряване на компютърно-човешките интерфейси на носимите устройства и потребителското изживяване. Това би могло да даде възможност на самите устройства да „научат“ (чрез методите на машинно обучение) поведението на потребителите, което не се основава само на времето, когато интерфейсът е активиран, но също така и разчита на позата на потребителя. Прилагането на такива алгоритми може да накара интерфейса на устройството да не следва предварително поръчаните и кодирани в операционната система на устройството или потоците от менютата на софтуера, а да започне с приложенията или настройките на устройството, които са типични за потребителя въз основа на разпознаване на потребителската поза. Това ще намали времето за взаимодействие с устройството и усилията на потребителя да изпълни необходимите задачи за въвеждане на устройството. Знаейки в каква поза е потребителят и през деня може да се управлява също яркостта на дисплея на устройството, цветовете на интерфейса, стила на иконите и т.н., за да се осигури по -добро потребителско изживяване и да се спести енергия на устройството.
Експерименталните данни показват, че за всеки две дадени пози (от трите възможни пози) би било възможно въз основа на позицията на пръстите на потребителите върху чувствителната на допир рамка на носимо устройство (интелигентен часовник) да:
• прави разлика между стоящи и седнали пози (Dsc) с 60% вероятност
• прави разлика между седнали и легнали пози (Dcb) с 80% вероятност
• прави разлика между стоящи и легнали пози (Dsb) с 90% вероятност
Изводът е, че легналата поза може да бъде диференцирана с достатъчно голяма вероятност, докато седящата и изправената поза в повече от половината от случаите (60%). Ако метода за разпознаване на пози се базира върху относителните „делти“, може да се постигне дори най-високата вероятност.
Представеният метод не е свързан с водещата потребителска ръка (с която потребителят работи с устройството си), така че описаната методология може да се приложи и към потребители, които носят устройството на дясната си ръка (съответно управляват устройството с лявата си ръка).

Г.8.16. Алексиева В., В. Г. Димитров, Десктоп приложение за обучение в кодиране на данни и визулизации на модулации, //Компютърни науки и технологии, ТУ-Варна, 2018, бр.1, с.39-45, ISSN 1312-3335

Предложеното настолно приложение реализира най-популярните алгоритми за компресиране на данни без загуба. То визуализира кодираните низове с основните модулации. Идеята е да се представи един и същи текст на съобщение в друга кодова схема и да се види как те изглеждат като модулиран низ в съответната преносна среда. Това приложение е изготвено с цел да се използва за визуализации в упражнения, свързани с кодиране в преносните среди при мрежови комуникации.

За представеното десктоп приложение за кодиране на данни и визуализация на модулации е избрана среда Microsoft Visual Studio 2012 и език за програмиране C#.

Функционалните изисквания към приложението са:

- да позволява на потребителя да въвежда своята информация (поредица от ASCII символи или числа) и на база на нея да се визуализира избраната модулация - амплитудна, честотна, фазова;
- да позволява на потребителя да въвежда своята информация, и на база на нея да демонстрира нейното кодиране по различни алгоритми - код по четност, цикличен код, код на Хеминг и код на Шенон-Фано;
- да позволява на потребителя да проверява и открива с приложението грешки на вече кодирана информация.

Нефункционалните изисквания са:

- интерфейса на приложението да е на английски език, за да се даде възможност да се използва в курса на обучение и на български, и на английски език
- опростен и интуитивен интерфейс
- автоматична визуализация на модулациите и резултатите от кодирането.

С оглед на целевата група, за която е предназначено приложението и съгласно заложеното в курса по “Основи на комуникациите”, където се ползва, са избрани стандартни алгоритми за реализация, като за реализация са предвидени основните видове модулации - амплитудна, честотна и фазова модулация, като фазовата модулация е с фаза 180^{o}. За реализация на кодиране на символи, представени с ASCII код в двоичен вид и на числа, преобразувани в двоична бройна система, са избрани код по четност, матричен код по четност, цикличен код с 5 различни полинома, код на Хеминг и код на Шенон- Фано.

Към момента се прилага в дисциплината "Основи на компютърните комуникации" в ОКС "Бакалавър" на специалност "Компютърни системи и технологии" както в обучението на български език, така и в обучението на английски език.

Г.8.17. Алексиева В., А.Хулиан, Крипто-токен базиран на смарт контракт на Етериум блокчейн, John Atanasoff Society of Automatics and Informatics, Sofia, October 4-6, 2018, ISSN 1313-1869, с.125-128

Настоящото решение се базира на Ethereum, защото позволява създаване на смарт контракти (smart contracts) и изграждане на приложения, които работят върху самия блокчейн. Смарт контрактът удостоверява, че участник “А” трябва да заплати дадена сума от сметката си на участник “Б”, който ще предостави на участник “А” определени услуги. Той се качва в блокчейна на валутата и копие от него има при всеки потребител на системата, така се извършва потвърждение на договора от хилядите миньори в нея. Смарт-контрактите се описват чрез нов програмен език, създаден за целта – Solidity. На 11.09. 2017 г. от Етериум е приет стандарт за смарт контракти EIP20 (Ethereum Improvement Proposal 20), съвместим с всички Етериум портфейли и платформи. ERC20 описва имена на променливи, функции и тяхната функционалност.
На база смарт-контрактите, Етериум предоставя възможност за изграждане на приложения и пълното им интегриране в блокчейна - dApps (Distributed Applications). Тези приложения са подписани и с електронните подписи на потребителите и само притежателите на частния ключ могат да отключат информацията която се намира там. За работата на тези приложения се изразходва GAS, а също и при изпълнение на код. По този начин разработчиците са стимулирани да създадат оптимален код и да предотвратяват безкрайни цикли.
Настоящото решение е разработено с Truffle и Ganache под операционна система macOS High Sierra. Truffle предлага интегрирана система за компилиране на написаните смарт контракти, както и скриптове за качване на контракта на Етериум мрежата. Ganache създава локален блокчейн на базата на Етериум, в който може директно да се изпълняват команди, както и да се провеждат тестове. Имплементацията на Етериум блокчейн е написана на JavaScript.
За да се създаде токен е необходимо да се опише какво е максималното му количество, да се създаде начин за проверка неговата наличност, както функции контролиращи прехвърлянето му от един адрес на друг. Това се осъществява чрез предложения смарт-контракт. Чрез конструктора се инициализира максималния брой токени и те се присвояват на адреса, от който е изпълнен конструктора. Той се изпълнява само веднъж от адреса, който го излъчва в мрежата. Събитията (Events) се използват за съхранение на информация в транзакцията. Записана веднъж, тази информация ще съществува, докато е видим блока, в който се намира транзакцията. При сегашната имплементация на Етериум, това значи завинаги. Записаната информация не е достъпна от смарт-контракти, дори и от този, който я е създал. Основното им приложение е при употребата на потребителски дефинирани JavaScript функции, които чакат настъпването на определено събитие, за да извършат някакво действие. В тази реализация - събитие “Transfer” отразява преместване на токени от един адрес, към друг, както и техния брой, а “Approval” извършва сходно действие, но дава разрешение от собственика на токените, те да бъдат изхарчени от някой друг.
Предложения смарт контракт е тестван с вградените механизми за тестване на Truffle и резултатите показват, че е напълно функционален.

Г.8.18. Алексиева В., А.Хулиан, Смарт контракт на Етериум блокчейн, UNITECH’18, 16-17 November 2018, GABROVO, vol.II, pp. 117-122, ISSN 1313-230X

В наши дни интелигентните договори позволяват извършването на надеждни, проследими и необратими транзакции без трети страни. Има някои възможни приложения на интелигентни договори, например в логистиката, управлението, банковата система, застраховането, имотите, IoT и други. Предложеният доклад представя прилагането на интелигентен договор, базиран на блокчейн на Ethereum. Децентрализираният крипто-токен е създаден за първоначално предлагане на монети (ICO) и е базиран на стандарта ERC20. Създаден е уеб-базиран интерфейс за продажбата на тези крипто-токени. Представени са резултатите от експерименталните тестове.

Настоящото решение е разработено с Truffle и Ganache под операционна система macOS High Sierra. Приложението изцяло спазва стандарт EIP20 и е използван специализираният програмен език за смарт контракти Solidity. За интерфейс на приложението се използва web3.js (JavaScript базирана библиотека, която позволява да се комуникира с мрежата на Ethereum и да се изпълняват смарт контракти). Клиентската страна на приложението изисква използването на добавка към съществуващ браузър Metamask.

За да се създаде токен е необходимо да се опише какво е максималното му количество, да се създаде начин за проверка неговата наличност, както функции контролиращи прехвърлянето му от един адрес на друг. Това се осъществява чрез смарт-контракт имплементиращ ERC20 стандарта, наречен от авторите AutoCoin. Вече качен смарт-контракт не може да се изтрива или променя, а се качва нова версия. Като глобални се декларират променливи за броя продадени токени, цена за един токен и администратора на смарт-контракта за продажба на токени. Цената за един токен е 0.01 Етера за токен.

Интерфейсът на приложението предоставя информация за броя токени за продажба, броя закупени токени, информация за адреса, с който потребителят се е свързал с него, както и наличното количество токени. Въвежда се количеството Етери, което ще бъде прехвърлено, таксите по транзакцията, максималния GAS, който може да бъде изразходван по време на транзакцията, като е възможно и ръчно да се въведе цена за GAS, представена в GWEI. Тази цена пряко влияе кога транзакцията ще влезе в блок. При цена от 40 GWEI е почти напълно гарантирано влизане в следващия блок, 20 GWEI обикновено означават включване в следващите няколко блока, при минималното количество 2 GWEI понякога са необходими няколко минути, за влизане в блок. Ако се зададе ниска стойност и транзакцията не влезе в блок, е възможно коригирането на цената към по-висока, за по-бързото изпълнение на транзакцията.

Представени са експериментални тестове, които доказват работоспособността на предложения смарт-контракт за ICO и управляемостта му през предложения web базиран интерфейс.

Г.8.19. Aleksieva V., S.Slavov, Managed active directory in directory-as-a-service, //Journal of the technical University of Sofia Plovdiv Branch, Bulgaria, Fundamental science and Applications, vol.24 ,2018, pp. 117-122, Plovdiv, ISSN 1310-8271

Тази статия представя разширена версия на доклада Г8.14.
Active Directory (AD) е една от последните категории, които правят преход към облака. AD като SaaS ще даде решение на IT администраторите могат да се възползват от синхронизация на локални директории и облака, като по този начин една и съща идентичност ще се използва и в двете среди.
В тази статия е предложена уеб-базирана система за управление на AD, която осигурява безпроблемно и просто изживяване на IT администраторите и синхронизира локални директории и облака, като по този начин една и съща идентичност се използва и в двете среди.
Разработената уеб-базирана система (MATEX) управлява AD. Сървърната страна се основава на скриптове и командлети на PowerShell. Системата е разработена с Visual Studio 2010, ASP.NET, C#и Windows Powershell.
За да се определи ефективността на MATEX се прилагат различни тестове, чрез симулиране на пригодността за работа за определен брой потребители, които използват сайта едновременно.
MATEX управлява едновременно заявки на 5, 10 и 15 потребители едновременно. В случай на 20 едновременно активни потребители, вече има наблюдавани моменти, в които производителността спада значително в определени моменти. Всички уеб страници и скриптове от MATEX се зареждат за приблизително еднакъв период от време за множество потребителски заявки. Средното време за множество „кликвания“ е измерено за различен брой потребители (5,10,15), направени по едно и също време и е много малко. За 20 потребители средното време се удвоява. Изводът е, че 20 е границата и на активни потребители, които използват едновременно MATEX, защото над този брой продуктивността и производителността му се намаляват.

Г.8.20. V. Aleksieva, A. Huliyan, H. Valchanov, An approach of Crypto-token for Smart Contract based on Ethereum Blockchain, Journal of the Technical University – Sofia, Plovdiv branch, Bulgaria, "Fundamental Sciences and Applications", Vol 25 No 1 (2019), pp.1-7, ISSN 2603-459X, https://journals.tu-plovdiv.bg/index.php/journal

Предложената статия представя решение за създаване на децентрализиран токен за прилагане на интелигентен договор, базиран на блокчейн Ethereum. Създаден е уеб базиран интерфейс за първоначално предлагане на монети (ICO). В експериментална среда бяха проведени изследвания за различни сценарии. Представени са резултатите.

Този интелигентен договор и уеб-базиран интерфейс са представени в Г8.17 и Г8.18. В тази статия са представени експериментални тестове и резултати за неговата функционалност.

Първата част от тестовете е свързана с правилната работа на интелигентния договор - баланс на сметката, прехвърляне на токени и т.н. Има няколко инструмента за автоматизирани интелигентни договори (написани на Solidity) за тестване на уязвимости на сигурността на базата на анализ на ниво код.

В подхода на Reza е дадено обобщение на четирите най-подходящи инструмента, които е възможно да се използват в експериментите, а именно Oyente, Mythril, Securify и SmartCheck. Въпреки това, степента на строгост на оценката, вариращa от синтактична, евристична, аналитична до напълно официална, се отнася до основната техника за тестване на сигурността на дадения инструмент и до този момент изследователите се доверяват на внедрените в инструменти за тестване на стабилността. Truffle (и Solidity) има вграден механизъм за тестване на интелигентни договори, написан на JavaScript, който тук се използва.

За директно тестване на трансфер, 250 000 токена се прехвърлят от адреса на администратора до адреса на получателя. След като прехвърлянето е извършено, събитието се улавя и проверява за тип „Transfer". Ако този тест е успешен, балансът на адреса на получателя се проверява за наличие на прехвърлени токени. Делегираната проверка за прехвърляне е подобна на проверката за директно прехвърляне. Първо, 100 токена се прехвърлят от адреса на администратора на адреса, от който ще бъде разрешен делегиран трансфер – адрес_1. Позволено е да се изразходват 10 символа от адрес_3, който ги изпраща на адрес_4. След извършване на тези действия, той се очаква адрес_1 да има 90 токена, адрес_2 - 0, а адрес_3 да е 10 токена. Показани са резултатите от тяхното изпълнение с грешни и правилни параметри.

В истинския блок на Ethereum е фиксирано времето за в блок, но има динамична промяна на трудността в зависимост от това колко енергия е включена в мрежата. Тестовете бяха проведени в локална мрежа с flat топология. Клиентът се свързва със сървъра Metamask. Параметрите на компютрите са Apple Mac Book Pro Late 2011 Specs, Core i5 (I5-2435M) 2.4GHz 2/4 ядра/нишки, 4GB DDR3 1333Mhz RAM. В Метамаск при изпращане на етер за закупуване на токен се използва протокол TLSv1.2. В статията е представена мрежовата комуникация между клиент и Metamask сървър по време на успешна транзакция на токени.

Г.8.21. В. Алексиева, Х.Вълчанов, А. Хулиян, Приложение на интелигентни договори базирани на Ethereum блокчейн за целите на застрахователни услуги, // Информатика и иновативни технологии, сс.7-14 бр.1(1),2019, ISSN 2682-9517

Настоящата статия представя експериментална реализация на интелигентни договори за застрахователни услуги върху Ethereum блокчейн. Авторите представят класически модел на застрахователна услуга и изтъкват неговите недостатъци. На тази основа предлагат модел за застрахователни услуги, базиран на блокчейн технологии. Представена е експериментална реализация върху Ethereum блокчейн.

Процесът на обработка на иск може да бъде подобрен, използвайки интелигентни договори и блокчейн технология. Информацията за настъпила щета може да се изпраща от застрахования или директно от сензори, монтирани в застрахования обект (smart asset), към автоматизирано приложение за обработка на иск. За съответните застрахователни политики, които се осигуряват от интелигентния договор (smart contract), клиентът ще получи обратно потвърждение в реално време. Искът се обработва автоматично от smart contract на базата на зададена бизнес логика, като се използва предоставена от застрахования информация. DLT автоматично използва допълнителните източници (статистики, отчети) за оценка на иска и изчисляване на щетата. В зависимост от застрахователната политика, smart contract може автоматично да изчисли персоналната отговорност. При известни ситуации smart contract може да активира допълнителна оценка на иска. Ако искът е одобрен, плащането към застраховани се инициира чрез smart contract.

Предимствата на новия подход, базиран на интелигентни договори върху блокчейн технология, могат да се разгледат в няколко аспекта. Изпращането на иска е опростено и автоматизирано. Благодарение на директния обмен на информация за щета между застрахователите, DLT премахва необходимостта от участие на брокери и редуцира времето за обработка на иска. Вградената бизнес логика в интелигентния договор в блокчейна елиминира необходимостта вещите лица да преглеждат всеки иск (с изключение на специфични ситуации). Застрахователят има достъп до историята за произхода на щетите, което помага за идентифициране на потенциални опити за измама. Използваната информация е интегрирана, благодарение на възможностите на DLT да обединява данни от множество доверени източници. Процесът на плащане на щетата е автоматизиран от интелигентния договор върху блокчейна, без необходимостта от използване на посредник.

Изложени са предимствата и недостатъците на използване на частен и публичен блокчейн, както и на комбинирани решения с 2 блокчейна (за автоматизиране на бек-офис операциите да се ползва частен блокчейн, а за управление на автоматичните плащания със съществуващи криптовалути или когато има нужда да се осигури доверие да се ползва публичен блокчейн).

Представеното решение е с публичен блокчейн Ethereum.

Г.8.22. В.Алексиева, Х.Вълчанов, Ю.Димитров, Study of smart watch interfaces, UNITECH’19,15-16 November 2019, GABROVO, vol.II, pp. 12-16, ISSN 1313-230X

Умните часовници са носими устройства с малки размери. Техният размер на дисплея и ограниченото пространство за контроли за въвеждане изискват специално внимание към процесите на разработване на интерфейси на устройството. Изследването в този доклад има за цел да сравни два различни подхода в дизайна на интерфейса - нов интерфейс, базиран на активиране и управление с два пръста на сензорен интерфейс на безела на устройството, чувствителен на допир (повърхността, която е около дисплея), със стандартен интерфейс за въвеждане в стил „ръчен часовник“въз основа на странични бутони.
Целта на това проучване е да се сравни процеса на взаимодействие човек– смарт часовник, когато един и същ потребител изпълнява една и съща задача при използване на два прототипа на смарт часовници, разработени за целта.
За целите на изследването са изработени два експериментални прототипа с различни входни интерфейси - „Нов“ с интерфейс с чувствителен на допир безел, който е разработен за предишно изследване, и „Стандартен“ с четири бутона отстрани на устройството, който е проектиран и разработен за настоящото изследване. За да са напълно сравними резултатите от изследванията, двата модела са изработени въз основа на един и същ 3D модел на ръчен часовник. Експерименталните модели се управляват от компютър Arduino Mega 2560. Разработен е софтуер за управление на всеки един модел на база на Arduino. И двата софтуерни продукта разпознават четири основни командни интерфейса за взаимодействие - „Нагоре“, „Надолу“, „Избери“ и „Назад“.
Тестовата група се състои от 10 доброволци, ползващи дясна ръка за работа с прототипите. Средната възраст на участниците в експериментите е 37,6 години. Всички експерименти са проведени при равни други условия - в едно и също помещение, без наличие на изкуствено осветление.
Изследването на разработените модели на интерфейси на смарт часовници се проведе в три етапа – на първия етап се сравняват времето и точността на изпълнение на проста задача (избор само на една функция), на втория етап се сравняват времето и точността на изпълнение на сложна задача (избор на функция в няколко стъпки), а на третия етап доброволците дават субективна оценка за комфорта на работа с двата интерфейса.
Представени са данните от експериментите.
Изводите от проучването могат да се обобщят в следните:
• Новият експериментален модел превъзхожда стандартния по скорост на работа. Когато наборът от команди е по-дълъг, ползата от използването на новия модел на интерфейс е по-голяма.
• Коефициентите на грешки при работа с новия модел са по-високи от тези при използване на стандартния модел. Причината може да е фактът, че традиционните интерфейси със странични бутони на електронен часовник са познати на повечето хора, но интерфейсът на новия модел с чувствителен на допир пръстен е нещо ново за тях.
• Оценката на потребителите за комфорта на работа с двата интерфейса е по-висока за работата със стандартен модел.

Г.8.23. Х.Вълчанов, В.Алексиева, Ж. Едикян, Study of wireless networks security, UNITECH’19, 15-16 November 2019, GABROVO, vol.II, pp. 7-11, ISSN 1313-230X

Безжичната мрежа позволява лесно изграждане на домашни мрежи и мрежи в малки предприятия, базирани на стандарта IEEE 802.11. Въпреки това, безжичните мрежи са лесно податливи на атаки срещу тяхната сигурност. Това изисква анализ на проблемите и създаване на препоръки за подобряване на тяхната сигурност. Тази статия представя методология и изследване на сигурността на безжичната мрежа във Варна. Информацията е събрана с помощта на техниката war-driving. Получените резултати се анализират и сравняват с тези от предишни проучвания.

Системата за събиране на данни е изградена на базата на едноплатков компютър Raspberry Pi 3 Model B, с процесор ARM Cortex-A53, 1.2GHz, вградена Wi-Fi и Bluetooth функционалност. За целта на реализацията е нужно записването на позицията на всяка безжична точка за достъп. Избраният GPS модул, поради поддръжка на стандарта NMEA 0183, дълготрайна батерия и голяма памет е Holux M-1200E. За сканиране на безжичните мрежи се използва модул CanaKit Wi-Fi Module. За да се осигури продължително захранване на едноплатковия компютър, се използва портативна батерия Canyon CNS-TPBP5DG с капацитет 5000mAh.

Сканирането на безжичните мрежи е реализирано посредством софтуер с отворен код Kismet. Софтуерът е компилиран и инсталиран под операционната система Raspbian OS. Получените от Kismet данни се записват в netxml формат. Събраната информация са конвертира чрез скрипт на Python в csv формат. Това е необходимо, за да могат данните да се представят в табличен вид с цел по-лесна обработка и анализ чрез Microsoft Excel. Избраният район за анализ включва централната част на гр. Варна, тъй като в нея се намират по-голяма част от офисите и голяма част от живущите. Също така, районът съвпада с проведено подобно изследване от 2008г., с цел сравнение на получените резултати.

Резултатите показват значително увеличаване на сигурността на Wi-Fi мрежите в града, но въпреки това има какво още да се подобри в тази насока.

Причините за подобряване на сигурността могат да се разгледат в две насоки. Първо, производителите предлагат устройства, които по подразбиране имат конфигуриран протокол WPA2. Второ, по-големите организации имат ИТ отдели, които се грижат за сигурността. Въз основа на резултатите за откритите SSID, смесен режим WPA/WPA2 и WPS, може да се заключи, че повечето от анализираните Wi Fi мрежи принадлежат на обикновени потребители, които нямат достатъчно знания за сигурност.

Основните препоръки могат да бъдат представени в следните направления:

1. Да се използва само метод WPA2 за криптиране.
2. Да се деактивира WPS за всички устройства.
3. Да се избира сложна парола.
4. Да се актуализира софтуера на устройствата до последната версия.
5. Да се информират потребителите за проблемите в сигурността на Wi-Fi мрежата.

Г.8.24. D.Dinev, V.Aleksieva, H.Valchanov, K.Genov, LoRaWan Network Mobility Software Simulation Tool, // „Компютърни системи и технологии“,бр.1,2021г, сс.31-38, ISSN 1312-3335

В този доклад е представен симулатор за реализиране на мобилност в LoRaWan мрежи. Някои от многото изисквания на концепцията за IoT са изпълнени в широколентови мрежи с ниска мощност (LPWAN) - ниска цена, енергийна ефективност и голямо покритие на зоната. Едно от най-проучените внедрявания на LPWAN технологиите са широкообхватните мрежи с голям обхват (LoRaWan). LoRaWan е сравнително нова технология с много предимства и недостатъци. Някои недостатъци могат да бъдат отстранени чрез изучаване на технологичните граници и създаване на симулатори, чрез които да се продължи по-нататъшното развитие на технологиите. В тази статия е предложен симулатор за внедряване на предаването в LoRaWan, който реализира мобилност на крайните устройства и намиране на най-добрия маршрут между крайните устройства преди и след това. Внедрените алгоритми за намиране на най-добрия маршрут между крайни устройства и симулиране на мобилност се използват за изучаване и подобряване на QoS параметрите в LoRaWan мрежи.

Мобилността (хендовер) в безжичните мрежи може да бъде причинена от много причини - физическо движение на свързаното устройство, промяна на характеристиките на мрежата и т.н. Има два различни типа хендовер в зависимост от вида на мрежата за достъп, която принадлежи на всеки PoA - хоризонтален и вертикален хендовер.

Симулаторът изпълнява мобилността в мрежата LoRaWan въз основа на предложения алгоритъм за мобилност. Качеството на сигнала се проверява за реализиране на мобилност. Стартирането на процедурата за хендовер се основава на стойността на силата на получения сигнал (RSS). Хендоверът се осигурява, когато бъде намерен друг gateway (терминал) с по-висока RSS стойност. Мобилността се осъществява на три етапа, съчетавайки предаване на слой 2 и слой 3. Симулационната среда има 6 блока: GUI (Графичен потребителски интерфейс) - включва лесен за използване потребителски интерфейс за симулации;Ядро - основен блок, изпълняващ всички операции на симулатора; Създаване на топология - блок за създаване на топология; Модификация на топология - блок за промяна на съществуващи топологии; Намиране на най-добрия път между крайните устройства - с помощта на „Depth First Search“ и „Hassle Free Route Algorithms“ може да се намери най-добрият маршрут между крайните устройства;

- Хендовер - с помощта на този блок мобилните крайни устройства се прехвърлят към новите терминални устройства, които отговарят на тези нужди във всяка тяхна посока на движение.

Бутонът „Char“ в раздела „handover“ отваря прозореца, в който могат да се анализират резултатите от извършените симулации. Представена е диаграма, показваща информация за крайните устройства - техния тип (мобилен, статичен) и състояние (активиран, деактивиран) за всеки терминал, също и диаграма, визуализираща броя на мобилностите, извършени между терминалните шлюзове. Представена е диаграма за MSN, обобщаваща и представяща броя на движенията за всяко мобилно крайно устройство, което е извършило мобилност и др.