РЕЗЮМЕТА НА НАУЧНИТЕ ТРУДОВЕ И УЧЕБНИ ПОСОБИЯ НА АНГЛИЙСКИ ЕЗИК

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"

B.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

In this paper is proposed a prototype for LiFi data communication and a comparison study of proposed by the authors LiFi prototype with other similar LiFi prototypes (P.Goswamis and LiFiNano). The limitations of the proposed prototype are:

- The maximum distance of transmission is when the LED bulb is at an angle of 90^o with horizontal plane. This angle guarantees the maximum transmit distance of 80cm. This result is achieved in a fully dark room.
- The more we decrease the angle of the LED bulb, the more the distance for successful transmission decreases. When the angle is less than 40o the receiving of data is unsuccessful.

The investigation of the proposed prototype focuses on the impact of some environment factors (as sunlight illuminance, glass border and saline water). As the experiments with the prototype have been made, its limitations for maximum transmit distance, under different environment conditions, are determined.

The goal of the current study is to collect data for transmission through different environment. A prototype, which was designed for previous research was used, but in software some enhancements are made, such as transmission speed and error correction improvements.

The direct sunlight (in this experiment—7520 lux) leads to 100% loss of the transmitted information to the receiver, even if it is 1 cm away from the transmitter. As much as we decrease the illuminance of the sunlight by moving away from the window, the distance Dmax increases. When reaching 2.5 m (200 lux), Dmax is 60 cm. The value of Dmax of 80 cm is reached on distance of 4.0 m from the window (where the impact of sunlight is 0 lux). This is the same as the maximum transmitted distance, which is reached in a fully dark room.

If the thickness of a glass border is only 2 mm, the distance is the same as the distance without a border. But if the thickness grows up, Dmax decreases. With glass border of 12 cm Dmax is only 40 cm—the half of the maximum distance.

Experiments with fresh and salt water (10% saline and 20% saline) were performed. Air is excluded, as the transmitter and receiver modules are stuck to the glass of the aquarium. On distance 55cm only 0% saline water accepts the communication, but on distance 26cm up to 20% saline water accept the communication.

The key performance indicators are chosen for the estimation and comparison of the prototype, subject of the above mentioned experiments, and other LiFi prototypes. Based on them, the comparison is made. The estimation is made with two complex criteria—average arithmetic and average geometric estimation. Regarding to the results of the evaluation, it can be concluded that the above mentioned prototype is the best option for the purposes of the present study.

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.

This paper examines the impact of the proposed by the authors traffic prioritization algorithm in LTE network, Round Robin (RR), Maximum Rate (MAX-Rate), Proportional Fair (PF), Exponential/Proportional Fair (EXP-PF), and these proposed by Myo and Akyıldız on the QoS in 4G LTE wireless mobile network.
The comparison based on the results of throughput, delay, packet delivery ratio (PDR) and packet loss ratio (PLR). To study the impact of traffic prioritization algorithms on QoS, the LTE simulation product proposed and further developed by the authors, is used.
Experimental studies were performed for static and mobile UEs for one LTE cell, for which transmit power is 40W (46.02dBm), 20 MHz bandwidth, noise power is -160.99dBm, 100 available PRBs, 6 sectors cell, and radius of 770m. Number of users used 20, 50, 70 and 100. Distance of static UEs to eNodeB (m) used for the studies are as follows – 10, 90, 170, 250, 330, 410, 490, 570, 650 and 730 (55m for all mobile UEs). Required type of service is GBR, required RBs from every UE are 5555 and pay price for guaranteed service with value 5. Movement Speed for Mobile UEs (km/h) used for the studies are as follows – 10, 20, 30, 40, 50, 60, 70, 80, 90 and 100.
The presented results show that with a smaller number of subscribers, the proposed algorithm provides higher values for the studied parameters for static subscribers located within a range of up to 250 meters from the eNodeB and provides higher values for the studied parameters for mobile subscribers moving at more than 80 km/h. With the increase in the number of subscribers, the serving becomes equable, but better values provided for the highest priority subscribers, while for the other algorithms the results are almost uniform.
The advantage of the proposed algorithm over others is that it serves with high priority requests from subscribers at a closer distance to the eNodeB and requests from mobile subscribers. Serving requests from subscribers closer to eNodeB improves the QoS because the channel quality of these subscribers is better and communication errors are less, which leads to faster service. Priority service for queries from mobile users improves the QoS because this reduces the loss of handover. Allocating more resources to the higher priority users will speed up the service of their requests and the resources released by them will be used to serve the low priority ones.

B.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.

This paper introduces a comprehensive comparative analysis between the suggested 6LoWPAN sensor network traffic prioritization algorithm by the authors and five standard sensor network algorithms. There are two main classes of traffic prioritization algorithms for sensor networks: Knowledge Free and Knowledge Based.
In the author’s algorithm, according to the prioritization initially, the highest priority scheduled requests containing Emergent Dispatch Header. This header identifies the packet as emergency. In the case of multiple Emergent Dispatch Header packages or ordinary packages, the requests from mobile devices are served with higher priority. When many movable devices are available their requests are prioritized, using their movement speed. With higher priority are served the requests from faster moving devices. In the presence of multiple mobile devices moving at the same speed, the next criterion on which the requests are prioritized is the distance of the sensor to the coordinator. For this purpose, the principle of the Knowledge Based, Least Weighted Farthest Number Distance Product First mechanism is used. Higher priority has the packets sent by the sensors closest to the coordinator. When there are many sensors at equal distance to the coordinator has many sensors, the requisitions are prioritized using the sensor's type of application. With the highest priority served, the Healthcare applications and then Security and surveillance, Environmental monitoring, Animal tracking, Vehicle tracking, Agriculture and Smart Buildings.
The authors create a simulator, which is used for investigation influence of the proposed and standard sensor network, traffic prioritization algorithms on QoS.
Comprehensive comparative analysis of the traffic prioritization algorithm proposed by the authors is presented for 6LoWPAN and five others. For complex comparison of algorithms for traffic prioritization in 6LoWPAN a system of criteria proposed. Comparison of traffic prioritization algorithms mainly based on the results of Delay, Throughput, Packet Delivery Ratio and Packet Loss Ratio. This comparison made for a specific type of traffic, for certain end nodes.
The suggested by authors traffic prioritization algorithm in 6LoWPAN is better than others investigated, according to average arithmetic and average geometric complex estimations.

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.

This paper introduces enhancements to the simulation product for 6LoWPAN networks proposed by authors, which enables service quality research. The influence of different algorithms for prioritizing traffic on throughput, delay, packet delivery ratio and packet loss ratio considered. The included algorithms in the software tool are proposed by the authors algorithm and other classic algorithms for prioritization: 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). The software tool provides an interface for evaluation of proposed and classic algorithms on sensor networks.

In the proposed simulator the number of sensor nodes operating in a given region can vary up to 100, depending on the size of the area to be covered. Devices in this area may be fully functional or reduced functional. Fully functional devices can work both as coordinators and as end nodes, while those with reduced functionality only work as end devices.

A 6LoWPAN sensor network simulated with one fully functional device that serves the requests of the end devices. The purpose of the research is to determine the effectiveness of the algorithms embedded in the simulator for prioritizing traffic and in which situations, for which nodes they improve the QoS.

The results of the proposed prioritization algorithm show that the values for the studied parameters are better for the static devices closer to the coordinator. Prioritizing requests from nodes that are closer to the coordinator in sensor networks is important, because they are networks of multiple devices that transmit data constantly. This causes interference in the communication environment and errors, which initiates the resending of packets. As a result, communication load and delay increases, and degrade the QoS. With fewer devices, requests with highest priority served with more resources - from the nodes located up to 6 meters from the coordinator. This speeds up serving for these nodes, while freeing up resources to use for low-priority devices and offsetting delays. In case of insufficient resources, the requests of the lowest priority devices postponed for service in the next time interval.

The results for the mobile nodes according to the proposed prioritization algorithm show that the values for the studied parameters are better for the nodes moving at speeds above 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.

An indoor test Li-Fi network implementation is proposed in this paper. The real network consists from three LiFi access points in the room for transmitting information at a distance of 2.5 m from the floor. Each of the LiFi devices is at a distance of 75 cm from the neighboring device. Maximum angle of illumination at which the devices transmit information 45^{o}.

The goal is to implement a user equipment (UE) Handover between LiFi access points of the physically constructed network, taking into account correctly and incorrectly received data during this process. The handover realization in Li-Fi networks is very important for increasing the reliability of the network and transmitting all the data before leaving the network.

The following experiments were performed:

- to determine the health of the network;
- to perform a handover of users from one access point to another neighbor;
- reporting of correctly and incorrectly received data;

During the experiments, the light in the room was averaged 16.6 lx.

The following parameters were used for the first group of experiments:

- number of sent characters – 10 000;
- movement speed of the user equipment – 1m/s, 2m/s and 3m/s
- distance between the transmitter and receiver (L) – 0.5m, 0.8m, 1m, 1.2m and 1.5m;

From the results obtained through the experiments it can be seen that at a normal rate of 1m/s all the data sent by the transmitter were successfully received without any losses or erroneously received packets when passing from one access point to another. This is the case for each of the measured distances between the transmitter and the receiver. As the speed increases, an increase in the percentage of incorrectly received or not received data is observed.

The following parameters were used for the second group of experiments:

- number of sent characters – 100 000;
- movement speed of the user equipment – 1m/s, 2m/s and 3m/s
- distance between the transmitter and receiver (L) – 0.5m, 0.8m, 1m, 1.2m and 1.5m;

From the results obtained through the experiments it can be seen that at a normal rate of 1m/s almost all data sent by the transmitter are successfully obtained. The losses are due to the fact that for this speed the device has already left the network range and has not received the rest of the packets. As the speed increases, more and more incorrectly received or not received data are noticed.

The results show that as the speed of movement of the user device increases and the distance between the receiver and the transmitter, the percentage of erroneously received symbols increases. The speed at which there are no errors during the handover in this test Li-Fi network is 1m/s.

B.4.6. Haka A., 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.

This paper presents enhancements to the ZigBee network simulation product for IoT proposed by authors in previous research. The main improvements of the simulation software are: ability to calculate values for Received Signal Strength (RSS) and Received Signal Strength Indicator (RSSI); visualising the contents of the IEEE802.15.4 frame in beacon-enabled mode; study of classic algorithms for prioritising traffic in sensor networks; study of parameters affecting QoS such as Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), Delay and Throughput.

As an improvement to the simulation product for ZigBee network, one Knowledge Free and one Knowledge Based algorithm for prioritising network traffic implemented. Knowledge Free algorithms process requests in the order of their arrival. Such an algorithm for prioritising traffic is First Come First Served (FCFS). Knowledge Based algorithms use either application information, network information, or both to prioritise traffic. The implemented Least Number of Hops First (LNHF) algorithm bases on knowledge of the network information. According to this algorithm, requests from the devices closer to the coordinator are served with high priority.

The construction of a ZigBee network realizes using a graphical user interface, through which the coordinators are created and end sensor nodes added to them. Parameters such as: number of connected end nodes, channel bandwidth, region, frequency, beacon order and superframe order are set for each Personal Area Network (PAN) coordinator. To specify and link the created simulation with the restrictions for a certain region in the world, an option for selecting a certain channel and visualising the operating frequency added.

When the coordinator and end nodes correctly added with the appropriate configuration, the traffic generated by the end nodes in the network prioritised. When prioritising the traffic according to the selected algorithm, the contents of five IEEE 802.15.4 frames filled in.

The results for static nodes from the tests performed show that the LNHF algorithm improves QoS for end nodes, at a distance of up to 7m from the serving device. This will speed up the work, as the interference at these nodes is less, because the signal from the coordinator is better, respectively packet retransmissions will be less.

The results of the tests with mobile nodes for the considered prioritisation algorithms are similar. For the devices moving at medium speed, the allocated resources are few and the values considered deteriorate. This can worsen the QoS for these devices, as the handling of their requests will be delayed, and an additional delay will be caused by the initiation of a handover when the device is out of range of current coordinator.

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.

This paper compares the results for the Received Signal Strength Indicator (RSSI) values from the end sensor nodes obtained by simulating a ZigBee network using the improvements to the simulation product presented in B.4.6. and through a real ZigBee sensor network.

Graphical user interface of simulator allows adding the coordinators and end sensor nodes for construction of a ZigBee network. Once the ZigBee PAN coordinators have been added, the end sensor nodes can be connected to them. The values for RSS and RSSI calculated immediately after setting the sensor distance from the coordinator. The changes for all inserted parameters reflect in the data tables and can check from the "Nodes Table" tab. The simulator calculates automatically the values for RSS and RSSI, based on distance between the added end sensors and PAN coordinator. The calculated values represented by graphs according to node's distance to PAN or node's ID.

The tests for RSS and RSSI from the simulator were obtained after building a ZigBee network by one coordinator (ZigBee router) and 6 ZigBee sensor nodes connected in a star topology.

The physical construction of the ZigBee network is done with BeagleBone Black – BBB01-SC-505 board with Bone-Debian-7.8 operating system working as ZigBee Gateway, Texas Instruments (TI) transceiver - CC2531EMK and TI multi-standard sensor nodes – CC2650STK. The ZigBee Gateway configured using TI Z-Stack Linux Gateway. The CC2531EMK board configured to operate as a ZigBee transceiver and sensor nodes to operate in ZigBee network using CC-DEVPACK-DEBUG of TI. The data transfer and the receipt of the RSSI values from the end sensor nodes in the already built ZigBee network can be tracked, when a second CC2531EMK transceiver configured to work as a ZigBee sniffer.

The results for the obtained RSSI values from the constructed ZigBee network are inconsistent in the tests for 2, 4 and 6 sensor nodes. The results of 2 sensors show that with increasing distance from the coordinator the obtained RSSI values deteriorate. This trend is not observed in the tests with 4 and 6 sensor devices. In them, with increasing distance from the coordinator, the obtained RSSI values are identical or better for some of the nodes and worse for others. This is due to the presence of external noise influences and interference between the sensor nodes, which can increase with the number of devices in the network.

The obtained results show that for 2 end devices in the network the values for RSSI obtained through the simulator are almost identical to those for the tests with a real network. The results with 4 and 6 end devices obtained through the simulator are close to those of the real network. The deviation in the RSSI values of the simulator is about 10dB compared to the actual results.

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.

This paper presents simulation software for studying QoS traffic prioritization algorithms in Li-Fi networks. In this framework are implemented algorithm proposed by authors from previous research, Wang traffic prioritization algorithm and two classic algorithms - First Come First Served (FCFS) and Least Number of Hops First (LNHF). The simulator calculates the packet delivery ratio (PDR), packet loss ratio (PLR), throughput and delay based on the allocation of resources through the implemented algorithms.

Proposed strategy for traffic prioritization distributes the resources in the terms of one timeslot, matches some criteria. The rearranging of the users connected to the Terminal according to the author's algorithm is the following: the users which are closer to transmitting point have higher priority and go higher in users table. If the distance from terminal to some of the users is equal, then the algorithm is looking for next criteria – is the client device mobile or static? The static devices have less priority. The mobile users have higher priority according to their speed. The higher the speed is the higher priority the device has. The type of requested service is the last criteria of the algorithm. Each one of them belongs to certain class which has different priority according to QoS parameters. There are four types of classes:

- Class 1 - contains services for Handover Calls, Link Recovery Calls and Voice Calls.
- Class 2 - contains Video Call services.
- Class 3 – contains services for Browsing, HDTV and Voice Messages.
- Class 4 - contains only Background Traffics services.

The new functionality includes availability for prioritizing connected users by implemented new algorithms, calculating their QoS parameters for PDR, PLD, Delay and Throughput, comparing the parameters by every algorithm and showing the transmitting matrix for each algorithm. The transmitting matrix for each algorithm can be shown after calculating and allocating the resources requested by connected devices. A new data table for storing the QoS parameter for each algorithm has been added. For easily comparing and studding the QoS parameters for every algorithm a graphic chart can be made for each of them.

The software realizes fully working simulation of Li-Fi network with terminal devices and connected to them users with their specifications. According to realized traffic priority and resource allocation algorithms the software can calculate the Packet Delivery Ratio, Packet Loss Ratio, Throughput and Delay which are important to providing better Quality of service.

According to those results a conclusion can be made that the algorithm which is proposed has better QoS indicator values than the others considered into this paper.

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

This paper presents the physical deployment of 6LoWPAN network and the study of throughput and end-to-end delay indicators, which compared with the results obtained through the 6LoWPAN simulation product presented in previous author's research.
The tests for throughput and end-to-end delay from the simulator were obtained after building a 6LoWPAN network by one coordinator and 6 6LoWPAN sensor nodes connected in a star topology. The coordinator configured to work on channel 25. Up to 6 end 6LoWPAN sensor nodes can be connected to the coordinator. All end nodes are static, perform the same type of application and located at the same distance from the coordinator (from 1m to 5m). The tests for reporting the values for throughput and end-to-end delay were made with 2, 4 and 6 sensor nodes connected to the 6LoWPAN coordinator. Once the coordinator and end node information added, a simulation performed to send a certain number of packets. After adding the packets to the send queue, the calculated values for end-to-end delay and throughput displayed.
The results of the conducted experimental studies are in large numbers, so they are summarised and presented in a table. Since the simulation product considers tests in ideal conditions, at different distances the values obtained are identical. The difference in the experiments performed is manifested in relation to the different number of sent packets.
The physical building of the 6LoWPAN network is done with BeagleBone Black – BBB01-SC-505 board with Bone-Debian-9.9 operating system working as 6LoWPAN Gateway, TI transceiver - CC2531EMK and TI multi-standard sensor nodes – CC2650STK. The data transfer and the receipt number of bits from the end sensor nodes in the already built 6LoWPAN network can be tracked, when a second CC2531EMK transceiver configured to work as a 6LoWPAN sniffer. This can be done on a Linux machine using Sensniff program for 6LoWPAN.
The experiments are made with 2,4 and 6 sensors with simulator and with real network in the same conditions. For example, the deviation in the simulated results with 6 sensors from the real ones for end-to-end delay is average 99% for 5, 10, 15 and 20 sent packets, and for throughput is 98% for 5 packets, 94% for 10 packets, 86% for 15 packets and 79% at 20 packets.
The results of real network tests are variable because the communication between the sensors and the coordinator is influenced by environmental factors such as electromagnetic interference, radio interference, packet transmission errors, other sources operating on the same frequency, interference between sensors, etc.
The obtained trend in the simulation results and real conditions are approaching, which gives reason to allege that the simulation product is suitable for purposes of education.

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

This paper presents the deployment of a physical Bluetooth Low Energy (BLE) sensor network for IoT and a study of the RSSI values derived from the end sensor units in the network.

The physical building of the BLE network done with RaspberryPi 4 Model B board with Raspbian operating system working as BLE master device, with built-in BLE transceiver and Texas Instruments multi-standard sensor nodes – CC2650STK.

The star topology by connecting the end sensor nodes and the master one was realised to examination the alteration in RSSI values. Different experiments with 1, 2, 3, 4, 5 and 6 static nodes performed, where for every one the nodes are located at distances from 1m to 10m from the master device. The examination of alterations in the received RSSI values for static sensor nodes located at different distances from the master device and for mobile nodes moving at different speeds done.

For 1 node the results show that as the distance of the sensor from the master device increases, the received RSSI values deteriorate. However the value at 10 meters is significantly better than the previous ones. Although only one device is transmitting on the communication environment which is not loaded, the decline in the previous values may be due to external sources of interference. The trend that at closer distance to the service device the obtained RSSI values are better is confirmed from the other tests with 3, 4, 5 and 6 sensors. The measured values for RSSI decline more and more when the distance from the master device and the end nodes number in the network increase.

Similar experiments were performed with mobile nodes. For the second node it is seen that the RSSI values are considerably lower. This is bred by the load on the communication environment and the emerged interferences. The trend when the sensors moving at a lower speed, the received RSSI values are better is confirmed from the other tests with 3, 4, 5 and 6 sensors.

Experimental results for the RSSI with static sensor nodes show that with increasing distance between the end nodes and the master device, the received values aggravates with considerable changes. Experimental results for the RSSI with mobile sensor nodes show that with increasing the speed of end nodes, the received values aggravate, but the change in the results is smoother.

For both static and mobile nodes sustained the tendency of aggravation of RSSI values with enlarging number of end sensor nodes in the network.

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.

This paper presents a simulation environment that allows study the influence of the implemented algorithms for prioritising traffic on parameters related to Quality of Service (QoS) in ZigBee network.
Proposed traffic prioritisation algorithm for ZigBee is a modification of the previous proposed by authors algorithm and is intended to work in star topology. The product improvements are the ability to study the influence of different algorithms for prioritising traffic on parameters closely related to QoS, as well as visualisation of the built network topology. The simulation product has a modular architecture, and the operation of the individual modules is controlled by its core.
The algorithm checks several criteria for prioritising traffic in a ZigBee network. It is first checked for packages that are marked as urgent. In the presence of such packages, they are served with the highest priority. When there are multiple emergency packets or they are missing, the traffic is prioritised according to whether it is required by a mobile or static device. Requests from mobile devices are served with higher priority. When there are packets from more than one mobile device, requests are prioritised according to the speed at which the devices move. Higher priority requests are served from devices that move faster. Another criteria for prioritisation with the same others is the distance of the sensor from the network coordinator. Requests from sensors closer to the coordinator are served with higher priority. When the sensors are at the same distance from the coordinator, their requests are prioritised according to the value of cost. The requests with higher cost value are served with higher priority. Finally, the requests are prioritised according to the sensor application.
The performed experiments aim to study the influence of the implemented algorithms for traffic prioritisation in ZigBee network on the parameters PDR, PLR, Delay and Throughput, which are important to ensure good QoS. The presented experimental results show that with increasing number of nodes the service of the proposed algorithm for prioritising traffic in ZegBee network becomes even. However, higher values are provided for the studied parameters for the nodes closest to the coordinator. This will improve QoS and speed up service for these devices. This will free up the occupied resource faster and allow the lowest priority requests from the most remote devices to be served faster.
In contrast, the service of the classical algorithms is significantly even, which loads the entire communication in the network and can lead to deterioration of QoS. In addition, providing more resources from the proposed algorithm for serving requests from higher priority nodes, unlike the classic ones, will extend their battery life, as power consumption is only in active periods, and their number can be minimised by speed up serving.

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)

This paper presents the realisation of an IoT sensor network with Texas Instruments CC2650STK sensors, which can be configure and operate based on ZigBee, 6LoWPAN and BLE technologies. Experimental studies of the parameters End_to_End Delay, Throughput and PLR for the three technologies have been performed. Based on the results of the experiments, a comparison of the same between the considered technologies is presented. The aim is, as a result of the research, to formulate recommendations for the most appropriate technology for building a sensor network for IoT with the used sensor nodes.

The experimental studies for the considered technologies are realised with different number of simultaneously connected in the network static sensor nodes (2, 4 and 6). The experiments include calculating the values of the parameters End_to_End Delay, Throughput and PLR, which affect the QoS, at distances between the serving device and the sensor nodes of 1m, 2m, 3m, 4m and 5m, when sending 5, 10, 15 and 20 packets. In order to ensure comparability between the obtained results for the studied technologies, a star topology was used in all experiments.

According to the obtained results, the values for End_to_End Delay increase with the number of end nodes in the considered technologies, as more time is required to serve the requests of all devices. As the number of packets sent increases, so do the values obtained for End_to_End Delay, as there are more requests for serving on the network. With ZigBee in most experiments, the minimum and maximum value for End_to_End Delay is better than 6LoWPAN and BLE. In addition, in most experiments, the values obtained for ZigBee are constant and do not change drastic with increasing distance between the end nodes and the serving device.

From the obtained results for PLR it can be seen that the values increase in direct proportion to the number of nodes in the network for the considered technologies.

The following recommendations can be formulated from the experiments and the results obtained:

- In applications where it is important that the values for End_to_End Delay are relatively low and constant; it is better for the CC2650STK sensor nodes to be configured to work with ZigBee technology;
- In applications where constant throughput values are required, it is better for the CC2650STK sensor nodes to be configured to work with ZigBee technology;
- When required to provide higher throughput with a larger number of nodes in the network, it is better for the CC2650STK sensor nodes to be configured to work with BLE technology;
- In applications where less packet loss is required, it is better for the CC2650STK sensor nodes to be configured to work with ZigBee or BLE technology, as the PLR values obtained are extremely close, with lower values obtained for 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

Nowadays, with the expansion and improvement of communication technologies, the services offered are increasing, such as broadband Internet of Things (IoT) technologies, and one of the most common IoT technologies is Bluetooth Low Energy (BLE).
This paper presents a simulation product for the study of the communication and messaging between Master and Slave in the BLE network, which can also be used in education. It can be used both to study the basic functionalities of the technology and during onsite or online learning.
The developed simulator in the Department of Computer Science and Engineering at the Technical University - Varna has a modular architecture. When loading the application, the main functionality of the core is started, which is adding the Master device and realising its program logic for processing the incoming packets and their corresponding protocol data unit (PDU) type, as well as waiting for adding a Slave device and monitoring its status (Standby, Advertising or Connected). The execution of the main functionality is controlled by the "AppController" class.
To obtain statistical information about the time in which the end devices in the network were in a certain state, the core turns to the Statistics module, which is managed by the class "DeviceStatisticsUtil". The processed information through the various modules is visualised through the built graphical user interface (GUI).
After adding Slave devices, each of them can be allowed to visualise the distance to the Master, removed from the network or change its status from Standby to Advertising. When the state of Slave is Advertising, it starts sending advertising packets on the channels intended for this (37, 38 and 39). With this, the Slave sends broadcast packets on the communication medium so that it can be detected by the Master in the range, and possibly connected to it. When switching to Advertising mode, the tracking of the packets transmitted on the communication medium also starts.
In order to compare the exchange of messages when establishing a connection, sending data and terminating the connection between Master and Slave devices in the BLE simulator and a real environment, a real BLE network is configured. To ensure comparability between the results of the real and simulated BLE network, an experimental topology of one Master and one Slave was realized.
During the simulation, some of the details of the communication were omitted in order to simplify the process in consideration and facilitate its presentation during learning. The simulator represents the main messages in the implementation of the process, which allows it to be used during the learning both on site and online.
The results show that the simulator can be used to present the highlights of the communication between Master and 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 is a long-range, low-power, low-bitrate, wireless telecommunications system, promoted as an infrastructure solution for the Internet of Things: end-devices use LoRaWan across a single wireless hop to communicate to gateway(s), connected to the Internet and which act as transparent bridges and relay messages between these end-devices and a central network server.

This paper presents simulation software for finding best route in LoRaWan networks.

Depth First Search is an algorithm for crawling or searching in data structures such as "tree" and "graph". To implement the algorithm, a vertex or node of the structure is selected, which is denoted as a root and the crawl starts from it. All subsequent peaks are visited sequentially in depth until reaching one, without heirs, after which a search is performed with backtracking until reaching a new end point or after the complete crawl - to the root. The original version of the algorithm was created in the 19th century by Charles Pierre Tremo to solve maze problems.

The simulator uses a modified version of the algorithm, which searches all paths only to one end device defined as a destination, to find all possible routes from a particular Personal area network to another network.

There can be several routes in a multi-hop networks with the same parameters. Initially, using Hassle Free Route the route is selected according to the parameter for the shortest path. Authentic value is included to prioritize the routes. The authentic value is stored in the routing tables of the devices as a negative, positive number or 0, where:

- negative number - there is a large loss of packets along the route;
- positive number - the route is smooth;
- 0 - default value; the route has not been evaluated.

A higher positive value indicates that the route is more successful than the others. It indicates the number of successful broadcasts on this route. For each successful transmission, the authentic value is increased by 1, and for each unsuccessful transmission, it is reduced by 1. When a fragment contains an emergent dispatch header, it is forwarded to the route with the highest authentic value. These fragments are prioritized and sent in the most preferred way.

The average time to send a 51 byte LoRaWan fragment is Ttrans = 6 ms, which includes the transmission time and the back-off timer.

The simulation framework has 5 main blocks- GUI, Core, Creating topology, Topology modification, Finding best path between end devices.

To make the test about finding the “Best Route” between end devices a LoRaWan network with 5 terminal devices and 4 end devices is made. Tests for finding best route between end devices are made and proved that the proposed simulator is fully functional and suitable for LoRaWan networks researches.

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.

The Internet of Things Li-Fi technology provides high speed, bidirectional and secure wireless access. This requires a research into the quality of service of this technology. This can be done by using simulation software that will minimize the cost and time for building such networks. This paper presents information about comparative analysis between author's proposed simulator and some of the most well-known simulators (OptSim, Veins VLC, NS-2,NS-3, MATLAB) to explore the quality of service on the Li-Fi Internet of Things networks. A system of criteria for performing a comparative analysis of simulators for the Li-Fi network is proposed. This approach to Li-Fi network research for IoT can also be introduced in education.
Existing simulators of Li-Fi networks have a number of disadvantages related to their operation and functionality. Here they are presented.
The proposed criteria for comparison of the LiFi simulators are:

- Modeling of different algorithms for traffic prioritization in LiFi
- Modeling of different methods for resource allocation
- Simulation of mobility
- Maintaining a GUI
- Visual presentation of the studied network
- Analysis of the obtained results
- Easy installation
- Scalability
- User/developer manual
- Programming language
- Memory usage
- License

According to the presented results of the study, due to the wide range of considered criteria, the most suitable for the study of Li-Fi networks are MATLAB, OptSim and NS-3. However, a separate study of the criteria shows that the proposed simulator by the author provides better values for the indicators: "Easy installation", "Memory in use" and "License for use", which are extremely important for educational purposes.
The criteria for comparison do not specify the criteria "Visualization of the transmission matrix", i.e. unlike the simulator suggested by the authors, none of the other simulators provides this capability. It provides comparable, with other simulators, results against many other criteria. This proves that authors' simulator is very suitable for training and educational purposes.

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

The ZigBee is one of the advanced technologies for managing of the IoT sensor networks, because it provides a high Quality of Service (QoS) and low power consumption. One possible solution to achieve the better QoS in these networks is to use an efficient traffic routing algorithm. This paper presents an improved simulation framework in which an algorithm for forming a ZigBee hierarchical topology based on priorities, allowing hierarchical routing, is implemented. The simulation framework provides an opportunity to analyze the results of the algorithm through a visual interpretation of the network topology.

ZigBee uses a mixed routing mechanism combined with hierarchical tree routing protocol (HRP) and ZigBee ad hoc on-demand distance vector (Z-AODV). HRP is an active routing method whose route information is established when the network is deployed and remains unchanged, except when the network structure changes.

In the simulation framework, the authors' algorithm for the formation of an energy-balanced ZigBee network based on priorities with a tree topology has been implemented. The ZigBee topology consists of a single coordinator (the tree root), multiple routers (branches) and end devices (leaves). In this algorithm, the pricing method is used to achieve the goal. In the algorithm, it is assumed that the routers serve only to build the topology, and do not function as end devices. Each router and end device has a willingness to pay value - the priority for end devices and an energy level for routers. The coordinator and routers have a charging rate value - a price that must be paid by the end nodes to connect to them. Therefore, the higher the value for willingness to pay, the higher the priority has the end device.With routers, the case is similar, the higher the value of willingness to pay, the more energy there is.

The developed simulation framework has a modular architecture. Simulating a ZigBee network requires working through two main windows. One of them for adding parameters for the coordinator and the other for routers and end nodes in the network.

The visualization of the topologies from the performed experiments for the implemented algorithm for forming a hierarchical topology in ZigBee network shows that with increasing number of routers the depth of the hierarchy in the constructed tree increases. In terms of energy balance, the algorithm for forming the hierarchy ensures that the routers with more energy are arranged at a lower level (closer to the coordinator). This provides better energy efficiency for routers, as more devices will be connected to those with more energy and fewer devices to those with less energy.

Experiments show that the implemented algorithm allows the construction of a balanced in terms of energy efficiency hierarchical tree topology.

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

This paper presents an experimental implementation of smart contracts based on Ethereum blockchain for insurance services. A decentralized crypto-token, based on ERC20 standard for smart contract, is implemented. A web-based interface is created for sales of these crypto-tokens. The results from the experimental tests are presented.
The classic claim process can be improved by using smart contracts and blockchain technology. Information of loss can be sent from the insuree or directly from sensors mounted in the insured object (smart asset) to an automated claim processing application. For the relevant insurance policies provided by the smart contract, the customer will receive a real-time confirmation. The claim is automatically processed by a smart contract based on business logic, using the information provided by the insuree.
This approach automatically uses additional sources (statistics, reports) to evaluate claims and to calculate loss. Depending on the insurance policy, a smart contract can automatically calculate personal liability. In certain situations, a smart contract may activate an additional claim assessment. If the claim is approved, payment to the insuree is initiated by smart contract.
The advantages of the new approach, based on smart contracts on blockchain technology, can be seen in several aspects. Claim submission is simplified and automated. Thanks to the direct exchange of loss information between insurers, this approach eliminates the need of brokers and reduces the time needed to process a claim.
The embedded business logic in blockchain smart contract eliminates the need for loss adjuster to review every claim (except in specific situations). The insurer has access to the origin of the loss, which helps him to identify potential fraud attempts. The process of payment for loss is automated by the smart contract on the blockchain, with no need of an intermediary claims agent.
The proposed solution with smart contracts for insurance is based on the ERC20 standard. It has been implemented experimentally on Ethereum blockchain. The results of the experiments show that the proposed solution is fully operational in terms of managing automatic payments on approved claims for loss.

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.

The paper presents a solution for creation of a smart contract based on Permission Blockchain, in particular Hyperledger Fabric.
The proposed smart-contract is implemented on the computer with AMD Ryzen 5 2600 with 6 cores/12threads, 3.4GHz, 16GB DDR4 3200Mhz and SSD Nvme 500GB Read/Write Speed 3,500/2,700 MB/s. The operating system is Linux Ubuntu 16.04 LTS 64bit. In addition, Docker Engine Version 17.03 and Docker-Compose Version 1.8 are used.
The Blockchain network topology is next: There is one company (R1), which has one order node (O1) and one peer node (P1). It works with two different companies - R2 and R3. Each one of them has own consortium with main company. They are implemented in two independent channels – C1 and C2. Each consortium has two peers – C1 has P3 and P1, C2 has P2 and P1. As the peer P1 works for main company R1, it participates in two channels. L1 is a copy of Blockchain of C1, L2 is a copy of Blockchain of C2.
The Blockchain business solution is implemented by providing a connection between its individual organizations, for storage and exchange of information, as well as for its processing. The data are visible only between the organizations that have access rights, for which channels of communication have been established between them. To maintain the correctness of the data during recording and storage, peers are configured within the organization to maintain the operability of the network.
The Blockchain network uses a Docker container for the implementation of the Hyperledger Fabric. It uses the tool Docker Compose for defining and executing of multi-container Docker applications.
Once the Blockchain network has been configured and started, the business logic that will be executed on it must be implemented. The chaincodes are created with the programming language Go.
The tests are presented with Hyperledger Explorer for Fabric 1.4.x under Linux Ubuntu.
The proposed implementation allows fast and secure migration of smart contracts between independent channels. Each channel has own business logic and it is invisible for participants in other channels.

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.

The paper presents an implementation of smart contracts for property insurance services, based on Hyperledger Fabric Blockchain.

The private Blockchain as Hyperledger Fabric Blockchain is the better solution for insurance business, because of its trusted nodes, there is no requirement for consensus protocol. The main advantages are the quick access to information, the cheaper transactions and the control on privacy level. Due to these facts, it is suitable and useful in many areas of insurance services.

In the presented use case, two channels are created: one for consortium 1 (Channel 1) of company Org1 (insurance company) and company Org2 (broker 1), and one for consortium 2 (Channel 2) of company Org1 and company Org3 (broker 2). Each channel has its own Blockchain, as well as smart contracts (codechain) that work alone with it. Each consortium has two participants. The two channels work in parallel with each other and they are not visible to participants outside those allowed by the rules of the consortium. A peer can contain a copy of the Blockchain and smart contracts of more than one channel.

The proposed smart-contract is implemented on the computer with AMD Ryzen 5 2600 6 cores/12threads, with Linux Ubuntu 16.04. In addition, Docker Engine Version 17.03 and Docker-Compose Version 1.8 are used. The name of the created smart contract is *mycc* and it is installed on Peer 0 on Org1 in Channel 1. In the implemented business logic, it is possible the client to change its broker. This means that his policy must move from one channel to another channel. There are two possible scenarios, after copying it – it will remain visible in Channel 1, and the changes made after copying Channel 2 will not be visible. The other scenario is that it will be deleted, so it will no longer be visible for Channel 1 participants.

The testing of the use case operability is performed by sending requests to the installed chaincodes and checking their correct execution. The Hyperledger Explorer tool is used to visualize the created network for this experimental use case. To find information about a person, who is written on the Blockchain network, the function *queryOwnerByName* from smart contract runs with the script.

Smart contracts provide the opportunity to create policies, monitor their status and through the business logic that can be described in them, to automate the process of processing insurance claims.

Through smart contracts it is possible to create an insurance policy, to determine the insurance risk, to execute of insurance claims. The Blockchain also optimizes the reinsurance process, as well as the operations of brokers. In areas, where supply-side monitoring is required, this new solution will improve the insurance process.

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.

This paper proposes a model which aims to reduce not only the overall load on the SDN network, but also to reduce the bandwidth and improve the routing mechanism on the SDN networks. It combines segment routing algorithm and load balancing mechanisms based on neural networks. The main purpose of this model is to investigate the most compatible neural network model for network load balancing and to minimize the network traffic between the controller and network devices.

There are different load balancing mechanisms in SDN, which uses two main approaches – static and dynamic load balancing. The shortcomings and problems with approaches and algorithms in related works are considered.

The model is developed as a cross platform SDN controller using C++ programming language. It implements the *OpenFlow* protocol and follows OS specific system calls for higher performance.

The system contains four main modules: *SDN controller module, Prediction module, Path compute module* and *Path encoding module.* Collected network parameters from the system are used to compute the optimal path based on neural network algorithms. The parameters are reduced to a single coefficient, which is then used for training and prediction purpose.

Using a Q-Learning algorithm, the process is split in two flows. First there are no data on which to make the prediction. To fill that data, the module starts to learn and receives a reward for every successful conjunction. Once the model is trained, the module can predict any flow change. Once the connection is established, the controller sends a status check packet to get the network information of the device.

When receiving the information, the controller stores it in a *Network Global View* database. After that, the controller and the switch start to exchange echo packets to track the connectivity between them. These packets are used to track the bandwidth of the device.

The prediction process monitors possible changes of the network load. If it detects such ones, it sends a signal to the *Path Compute Module*, to update the Flow Tables with needed routes to make the network load balanced. Once the optimal paths are computed, they are sent back and installed to the switches. The controller also notifies the Prediction process of dropped network devices, which will automatically trigger the Flow table changes.

The proposed architecture model combines neural network algorithms with segment routing for achieving better performance and network load balancing. It improves the QoS and provides ability to predict overload of network routes.

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.

This paper presents an experimental implementation of smart contracts based on Hyperledger Fabric Blockchain for insurance services in comparison with another implementation of smart contracts based on Ethereum Blockchain.
The use case is the same in each implementation: the insurance company (Org1) works with four companies – Org2 (broker 1), Org3 (broker 2), Org4 (broker 3), Org5 (broker 4). Each consortium has two participants – an insurance company and one broker company. The company Org1 has its own peer Peer0, provided that it participates in four consortia and has copy of four smart contracts. The Peer0 has main role in the insurance process, because he administrates the relations between insurance and broker's companies in each consortium.
The proposed solution was developed with Metamask, Truffle and Ganache under the MacOS High Sierra operating system. Ganache creates a local Blockchain based on Ethereum, which can directly execute commands as well as perform tests. Metamask is used, as there is no need to download a local copy of the Blockchain. A connection to a site makes a connection with Ethereum. Metamask takes care of all requests from and to the Blockchain network. Metamask can perform the Ethereum wallet function and support sending and receiving Ethers and ERC20 tokens. Truffle is used for the implementation of the smart contract. It is an integrated system for compilation of the written smart contracts, and it uploads them on the Ethereum network.
The same use case in Hyperledger Fabric is based on four channels. The proposed smart-contract based on Hyperledger Fabric is implemented on the computer with processor AMD Ryzen 5 2600 6 cores/12 threads and with operating system Linux Ubuntu 16.04. In addition, Docker Engine Version 17.03 and Docker-Compose Version 1.8 are used. The main difference from decision, based on public Blockchain, where the network exists, is that in private Blockchain the first step is to create the Blockchain network.
The proposed public solution with smart contracts for insurance is based on the ERC20 standard. It has been implemented experimentally on Ethereum Blockchain. The results of the experiments show that the proposed solution is fully operational in terms of managing automatic payments on approved claims for loss. In the proposed Smart contract, the business logic is more complex and the solution is more expensive then solution, based on private Blockchain, because it needs to pay for computing power with "ETH" tokens.
The proposed private solution with codechains on Hyperledger Fabric is more flexible, more secure, faster, and cheaper than previous public solution.

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

The paper presents a comparison study of the proposed prototype for two fingers touch interface for smartwatch with two other prototypes.
In order to be observed the touch areas on the bezel, a dedicated 3D model is designed and printed. It is as close as possible to real smartwatch according to its size and form.
The first step is to choose the dimensions of the 3D model. The diameters of the real smartwatches vary between 34.5mm and 58mm, but 73% of them are between 42mm and 46mm. The height of the real smartwatches depends on kind of functions, but vary between 10,9mm and 16mm. Almost 80% of them are between 14mm and 15mm. Based on this statistics, the chosen dimensions of the 3D model are - diameter: 44mm, height: 15mm, bezel angle: 450, bezel width: 4mm; color: white; material: PLA.
The second step is to evaluate in which two separate and distinguished sectors on the device bezel is possible to be registered in order the device interface to be activated and further interface actions to be performed. The detailed results from this evaluation are presented from authors in other research.
The third step is to activate some functions with this touch sensible bezel prototype and to compare its functionality with a prototype with buttons. The authors made this comparison in other research and the main conclusion is: the touch prototype outperformed the prototype with buttons in speed of operations, especially when the set of the interface commands is longer.
The final step is to evaluate the prototype in comparison with the similar prototypes. In order to perform a comparative analysis of the author's prototype with others, the same criteria for evaluation are used. In Oakley's prototype, physical contact with the device edge was integral to the vast majority of inputs – only 17% are with two fingers. Participants also favored their dominant hands and use of their thumb and index fingers. The authors gave the results for eight ordinal directions, but in this comparison only results for matching direction is used. In Yeo's prototype the authors use multiple fingers to move the whole prototype, which is with a typical smartwatch size. They showed that their prototype is competitive with commercial smartwatches of this size while input events are generated responsively (55-61ms) and accurately.
The experimental data for authors' prototype are presented in comparison with Oakley's prototype and Yeo's prototype in the table. According to the results obtained for the complex evaluation, the prototype for two fingers touch interfaces for smartwatch proposed by the authors is better than two others. The main advantage of the proposed prototype is its standard size and less touch time in long sequence of touches.

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.

The purpose of the presented study is to propose a method for recognizing the pose of the user (lying, sitting, standing) when waking a wearable device from sleep mode, and the device interface to be activated in order to visualize information and execute some commands due to deliberate touching of the bezel on a wearable device with two fingers by the user.

If the pose is successfully recognized when activating the wearable device interface, quick access to features and applications in the context of the pose (those most likely to be performed by the user) will be offered. This will reduce the active mode time of the device, which will extend the period between two charges of its battery. Body pose recognition can be combined with other factors such as the time of a day - for example, in a lying position in the evening to offer quick access to some functions and applications, and in the morning, again in the same position to offer the user quick access to other functions/applications. Another factor may be a previous pose and/or activity - for example, in a standing pose immediately after getting up to offer quick access to some functions/applications, and in the same pose, but after a long run, to offer others. Thus, pose recognition when activating the interface of a wearable device will reduce the time to work with it, which will lead to a longer period between two charges of its battery. Deliberately touching the device activation bezel with two fingers cannot be recognized by any other action and an unsolicited quotation of the device may occur.

The recognition of the pose of the user's body is based on the relative difference in the position of the fingers on the bezel when activating the interface by him in the different positions of his body when using a wearable device. For this reason, it is not necessary to measure the angles in the same position for different users, as well as to determine specific areas of the bezel to determine the position of the body. It is sufficient for each device / user to establish (after starting to use the device) the different areas of contact when activating the interface and on the base of these differences to predict in what position the user's body is most likely at the time of activating the interface.

The experimental group consists of 10 people, all with a leading right hand, all participating voluntarily in the experiment. There are made 300 attempts - 100 for each body position.

Based on the results of experimental studies, it can be assumed that the proposed method for determining the pose of the user's body on a wearable device based on the location of the fingers of his leading hand on a touch-sensitive bezel on a wearable device, is effective and applicable.

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.

This paper presents a comparative analysis of the investigated solutions for distance learning in computer network subjects.

Compulsory social isolation during a pandemic posed new challenges for the system of education. The indispensability quickly moves to a remote form of education necessitated the use of a different educational approach. During a full lockdown, three approaches for training in classes related to computer networks were used and studied - simulation products, real computer network with remote access and virtual computer network with remote access:

1) To use simulation products as Packet tracer, GNS3 etc.
2) In the Department of Computer Science and Engineering at the Technical University- Varna is developed from authors a real computer network laboratory with remote access. The remote access is implemented through web management system, developed by authors. Citrix XenServer has been chosen as a virtualization platform, which has high performance, easy maintenance and is free to use. The main idea of laboratory design is to create a snapshot of the virtual machine (for the respective operating system) for each of the computers, using Xen's snapshot capability.
3) To achieve high flexibility and to avoid some disadvantages of a previous solution, an experimental virtual infrastructure has been implemented. It is based on two Sun Fire Z20 server machines connected to a 1G Ethernet network and using VMware ESXi. The choice of VMware Infrastructure 3 is dictated by its capabilities for multiprocessor support, dynamic balancing and resource allocation between virtual machines, as well as migrating virtual machines between individual servers without interrupting their operation. Based on the virtual infrastructure, a number of virtual machines with respective operating systems have been launched. The virtual infrastructure can be accessed with the VMware vSphere Client software.

The goal of the study is to evaluate which solution is more appropriated for distance learning in the student courses related to computer networks. A system of criteria for evaluating the studied solutions is developed, according to the challenges in online learning.

The comparison is based on a proposed by the authors system of criteria, consistent with the challenges of distance learning. In order to ensure objectivity in the comparison, a complex assessment of the considered approaches is performed, based on complex arithmetic estimation. According to the results from an average arithmetic estimation, the most appropriated solution for distance learning is determined to be using a virtual network infrastructure.

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)

This paper presents a solution, based on smart contracts on a Blockchain, whereby the insurer pays directly to the hospital for the services provided in favor of the insured and only if the sum insured is insufficient, the patient pays the hospital.
The disadvantages of the classical process in Bulgaria from the point of view of the insuree are:
•The person must pay directly for his/her treatment, which will be reimbursed in weeks or months.
•At a time when a person's health is a top priority, s/he has to provide documents and visit an insurer to reimburse the costs incurred by him, sometimes repeatedly.
To avoid these shortcomings, the solution proposed in this paper is with a smart contract on a Blockchain. The steps of the process are:
1. The illness/accident of the insuree, for which treatment has to be applied.
2. The treatment includes medical examinations, hospital treatment, outpatient treatment (prescription drugs, monitoring of the condition of the insuree by the GP, control examinations by specialists).
3. In case the person is obligatory insured and / or voluntary insured for the payment of the treatment, a smart contract is executed, which checks whether the person is insured (if yes – it orders the coverage of the amounts by the NHIF, according to an approved list of amounts it covers, as for the rest of the treatment amounts checks the available insurance amounts for the person and orders the coverage of the amounts by the respective insurer, entering in the policy of the insured the spent amount and only in case the treatment amount cannot be covered by NHIF and insurer, the person pays extra with direct payment.
The proposed implementation is based on Hyperledger Fabric. For each insurance company is created own channel (consortium). Each channel has its own blockchain, as well as smart contracts (codechains) that work alone with it. Each consortium has two peers – Peer0 from Org1 and another peer from insurance’s company. The four channels work in parallel with each other and they are not visible to participants outside those, allowed by the rules of the consortium. Peer0 has separate copies of the four blockchains. The business logic of the blockchain network is implemented by language Go.
With the proposed decision, the insuree will avoid direct payments. It will reduce paperwork, will eliminate the need for an expert for the insurer, which will reduce its operational costs and the risk of one insurance event to use two policies with overlap rather than supplementation. The experimental results are presented, which prove the applicability of the proposed solution.

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)

This paper presents a cloud-based system for booking appointments for clinic examinations and remote consultations. A comparison is made among three different solutions. The experimental results show that the proposed cloud-based solution is the best option in terms of response speed, scalability, easiest administration and cost-effectiveness.

The authors proposed web-based system *CollosalClinic_Online.* For implementation are used different tools and frameworks such as C#, HTML, CSS, JavaScript, Bootstrap, jQuery, Google API, ASP.NET. The development is in the integrated environment MS Visual Studio 2017, and the management of the relational database is with MS SQL Server 2019. The web server is Apache 2.4.46, and Internet Information Services 10.0 is used for web application and a site management, containerization and fast Cloud integration. It is tested on a local computer.

The second implementation is in the distributed environment with a platform VMware Workstation Pro v.12.5.1.

The third implementation is in the cloud Azure CDN. The application is accessed via the Internet with an URL generated by Microsoft Azure with an Azure domain, *https://purple-forest-09d81c203.azurestaticapps.net*. Microsoft Azure allows to build a dashboard to monitor the resources and performance of the system. A basic Dashboard is formed, in which all the necessary graphs for a real-time monitoring are built and adjusted.

A comparison was made among the three implementations. The results show that the Cloud based solution is the fastest, most efficient, it has excellent performance and fault tolerance. After comparing this solution with five other existing solutions for booking of medical examinations and according to the results of measuring loading time, downloading resources and the number of requests to the servers where the applications are hosted, Cloud implementation of the proposed system has the best performance indicators.

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)

In this paper is proposed different important criteria for implementing a comparative evaluation of traffic load balancing. At the end it is presented a complex comparative analysis of static and dynamic routing algorithms for traffic load balancing and QoS improvement in SDN. For static routing, three algorithms were compared – Open Shortest Path First algorithm, shortest widest path and simple routing with link detection proposed by the authors in other research. For dynamic routing three algorithms were compared – Extended Dijkstra's algorithm, Enhanced Interior Gateway Routing Protocol and dynamic routing with complex weights also proposed by the authors.

The experimental study and results are obtained under Windows OS, and Mininet simulator is used to simulate network topology and network traffic. On the same host OS where the controller is running, the Mininet simulator is ran as Virtual Machine. For the purpose of experimental study, the controller is developed using C++ programming language and implements OpenFlow for managing SDN network. The controller supports the main functionalities for managing SDN network and have in place implemented Open Shortest Path First, simple routing with link detection and dynamic routing with complex weights algorithms.

The controller implements all up to date versions of OpenFlow communication protocol and have modular design. It stores the global network view in operational memory and has the ability to install flow rules on network resources, as well as process each packet independently using packet in and packet out messages. The controller has the ability to detect switch accessibility using echo messages, which are exchanged each 5 seconds. It also supports ARP messages to discover connected hosts to network resources and stores their MAC addresses in operating memory by mapping the host to the corresponding switch with which it has a physical connection. The tests are made with different topologies for each routing algorithm.

The authors propose the system of criteria for comparison and complex evaluation of these routing algorithms. If the criteria are observed separately, it can be seen that the proposed by authors static routing algorithm does not provide good results for "Network load" compared to the two other algorithms, but it has equal results with them for supporting all network topologies. Also, observing the criteria of dynamic routing mechanisms shows that the proposed by authors algorithm has equal results for "Packet drop rate", "Topologies" and "QoS support". Due to the wide range of criteria in the complex assessment, the overall score for geometric and arithmetic complex estimation of both proposed by authors algorithms is better than the algorithms with which it is compared.

Г.7.12. D. Todorov, H. Valchanov and 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

In this paper is proposed a shortest path routing algorithm with dynamic composite weights in SDN networks using OpenFlow protocol. The algorithm choses the less loaded path based on dynamic node and edge weights by observing link loads between switches. In order to discover the network topology, the algorithm uses LLDP to find links between switches and relies to ARP messages to find hosts linked to switches. By this way it can perform routings through ghost switches, which does not support OpenFlow.

The experimental study is performed under Windows OS, and Mininet simulator is used to simulate network topology and traffic. The Mininet simulator is running on a Virtual Machine on the same host machine where the controller is running. The controller is developed using C++ programming language and implements OpenFlow for SDN management.

The examined routing algorithms are:

- the authors' Simple routing algorithm with link discovery between source and destination hosts from our previous work;
- Dijkstra's routing algorithm which routes the traffic based on minimum hop count;
- Proposed shortest path routing algorithm with dynamic composite weights.

The experimental results show that the algorithm performs better compared to Simple routing and Dijkstra's routing algorithm. During the topology discovery phase, it shows less network traffic even with the use of LLDP. This is due to a huge exchange of ARP messages between the switches used by Simple routing algorithm to link network devices. Also, the algorithm successfully achieved is main purpose to load balance the network traffic and provide better QoS.

It has a little increase of the latency during packet transfer, but this is due to a packet flow changes during the routing process in order to prevent congestions. During the experiments, all three algorithms have zero drop rate and all packets were transferred successful. In addition, all of examined routing algorithms have successfully processed network loops and have low use of memory and processing power from the controller.

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.

In this paper we present a simple routing algorithm with link discovery between source and destination hosts in SDN networks without taking into consideration the link cost. The algorithm reduces the messages passed between network devices and the controller, as well as the path computation for the flows. For the implementation and testing we have developed an OpenFlow controller which performs the main interactions with network devices and use Mininet emulator to perform experiments.
The system contains two main modules: SDN Controller module and Path Compute module. The SDN Controller module supports the main communication functions between the controller and switches. It stores information about connected devices and their flow tables in Global Network View database. To establish a connection between the controller and the switch, handshake packets are exchanged. After establishing a successful communication, the controller periodically sends echo packets to track switch accessibility.
The Routing module is responsible to find destination address in flow entry table and to provide the next hop for the packet to the controller. It doesn’t take into consideration the network load to achieve load balanced traffic. The module takes into consideration the first served ARP message based on which makes the decision where to redirect the packet.
The experimental study is performed under Windows OS. To simulate network topology and traffic Mininet simulator is used. Mininet is running on a Virtual Machine on the host machine. The controller with routing algorithm is running on the host computer. The controller is developed using C++ programming language and implements OpenFlow for SDN management.
The experimental results show that the algorithm achieves its main purpose to reduce the network traffic between the controller and network devices during the discovery phase. The algorithm doesn’t use Link Layer Discovery Protocol (LLDP) to find connections between network devices. By this way it eliminates the additional traffic and preserves the network bandwidth. The algorithm has zero drop rate and all packets are transferred successful. It also shows low times on transferred packets. Another advantage is successfully processing of network loops in mesh topologies and the lower use of memory and processing power from the controller.

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

This paper presents a system for generation of network DoS attacks, using protocols of TCP / IP suite - UDP, TCP and ICMP. The purpose of the developed system is for education and it offers versatile tools for simulating different types of attacks. DoS attacks with various parameters are implemented.

For realization of the proposed generator of DoS attacks is selected operation system - Kali Linux 2.0 sana, because it is optimized for performing penetration tests and many of the restrictions imposed by other popular Linux distributions and in most versions of Windows (except Windows XP / 2000 / Server 2000/2008), with respect to the RAW socket, are absent. The selected programming environment is Code Blocks 10.05, with the compiler GNU GCC.

To prevent possible abuse with this proposed noncommercial generator many restrictions are implemented as:

- Prohibition of multiple instantiation of software – starting it in parallel processes;
- Limit the maximum number of simultaneously working threads to 500. Each tread after 500 will wait in the FIFO queue to be started;
- The number of implementations of various types of attacks is reduced to four most popular attacks - flood with UDP packets, flood with TCP packets, flood with ICMP packets (there are two realizations - Ping of Death and broadcast attacks), flood with TCP SYN messages;
- The maximum total number of bytes sent to the "victim" will be limited to a maximum value of type unsigned long, regardless of the duration of the attack;
- Maximum size of a single ICMP packets is 64 bytes;
- The data buffer of UDP and TCP packets is limited to 27 bytes.

The proposed generator of DoS attacks provides the following features:

- set of popular DoS attacks to perform simulation tests;
- set of tools for customizing the parameters of the attack;
- tools for automated tests in order to re-simulation of various scenarios with minimal user intervention;
- good performance and high level of control on the performed tests;
- low system requirements;
- the most simple and intuitive set of commands;
- creation of log files for analysis.

The results of tests for each kind of network attacks (UDP/ TCP flood attack, ICMP flood attack, SYN flood attack) are presented. Tests are provided in two similar experimental situations - the attacked machine at the first situation is running under Linux Slackware, and at the second - under Windows 7. Tests are provided in the local Ethernet network.

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.
(Haka A. ,V.Aleksieva, Software model for allocation of bandwidth in passive optical networks//Computer science and technologies, TU-Varna,2016,No1,p.45-51, ISSN 1312-3335.)

In this paper is proposed a software simulation for analysis of the efficiency of allocating bandwidth in passive optical networks. An algorithm is presented for resource allocation in two stages for maximum utilization of bandwidth using orthogonal frequency multiplexing in the passive optical networks (OFDM-PON) - first it is allocated time interval (timeslot) for each subscriber unit (Optical Network Unit - ONU) and second sub-channels are arranged, where each of them consists of a group of subcarriers. Implementing the proposed approach based on dynamic allocation of subcarriers channels provides efficient allocation of bandwidth and reduces delays in transmission of requests of individual users.
The PON network consists of a centralized Optical Line Termination (OLT) on the ISP side and multiple Optical Network Unit (ONU) devices on the user side. ONUs share resources in a common optical stream that connects them to OLTs. The PON system must implement an appropriate MAC mechanism to ensure efficient transmission, efficient use of network resources, arbitrage access to the shared environment and avoid data collisions.
In the present development, an algorithm for resource allocation in two stages for maximum utilization of the connection capacity by using OFDM-PON is presented. OFDM-PON uses a synchronous frame structure to provide differential service to requests. When allocating resources, the proposed algorithm first allocates the time slot for each ONU and then arranges the subchannels (subcarrier group). This algorithm must meet two constraints:
• calculations for the allocation of resources are made for a single frame;
• One ONU uses only one subchannel to send to OLT data for multiple services within the frame duration.
The proposed algorithm is applied only in the upstream direction and is implemented in two phases:
1) Time slot allocation - assigns a temporary subchannel for each ONU
2) Redistribution of subchannels - the temporary subchannel j for ONU [i, j] will be replaced by a confirmed subchannel in which there is enough resource to deploy ONU [i + 1, j], thus minimizing the number of delayed for next frame resource blocks, and the bandwidth is compressed, i.e. no free trays remain.
To analyze the bandwidth allocation algorithm proposed in the present study, a traffic model for several OLTs is created, but visualization of the transmission matrix is performed only for an optional OLT.
A database has been created for storing the data from the individual experiments for the individual OLTs and for the users connected to them.

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
(V.Aleksieva, Simulation framework for realization of priority-based Zigbee network, John Atanasoff Society of Automatics and Informatics, Sofia, October 4-7, 2016, ISSN 1313-1869, p.125-12)

The paper proposes a modified algorithm for building a priority-based and energy-balanced Zigbee network. The modified algorithm determines the priorities of the devices through the pricing method, where the priority of the end devices and the energy level of the routers appear as a cost they are willing to pay. On this basis, an efficient energy-balanced prioritized tree structure of Zigbee devices is built.
In this method, it is assumed that the routers serve only to build the topology and do not function as an end device. Each device (end device or router) has a payment field, which is a priority for the end devices and an energy level for routers. The coordinator, along with the routers, also has a charging rate field that must be paid to connect to them. Therefore, the higher the solvency of the terminal device, the higher the priority. With routers, the higher the value of the solvency, the more energy they have, therefore they have to stay at a lower level in the hierarchical tree in order to be able to serve more devices.
When an end device has a higher value of payment than the value of its prospective parent, it connects to it, changing its price. In this modified algorithm, the routers are connected first so that they can build the network, and then the end devices are connected to them. When a router connects to a router or a router connects to the coordinator, the price of the parent does not change. In the event that a device with insufficient value of payment remains, it connects to the router with the smallest number of children.
A simulation environment has been created for the implementation of the proposed algorithm, which allows visualization of the Beacon-Only-Period method of transmission between devices in Zigbee tree topology of the network. A database has been created to store the data from the individual experiments for the coordinators and the devices connected to them. In order to ensure the universality of the created simulator and due to the fact that there is no uniformly approved translation of the terminology related to ZigBee, the language English was chosen for the implementation of the simulator. The time diagram shows the transmission of packets by the Beacon-Only-Period method to avoid direct collisions. This simulator offers the ability to build any real topology, which also consists of end devices.
A comparative analysis of the average packet transmission rate for different transmission durations over Zigbee network, created by the classical method and by the pricing method, is made. There is an improvement in the average speed in the Zigbee topology built by the second method.

Г.8.4. Митев З., 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
(Mitev Z., S.Valchanova, V.Aleksieva, Custom monitoring and management of virtual infrastructures based on Zabbix, Session Schedule&Abstracts, 55th Annual Science Conference of Ruse University, Smart Specialization-innovative Strategy for Regional Economic Trransformation, Rouse, 28-29.10.2016, University of Ruse Publishing Center, p.163, ISSN 1311-3321)

This is abstract of the awarded paper Г8.7 with "The best paper" in an anniversary book of RU.
In this paper are proposed tools for monitoring and management of virtual infrastructures based on Zabbix- monitoring of websites, filling in host's information, monitoring of processes in Windows services, sending of notifications to Gmail customers, monitoring an Apache server, monitoring the size of the Recycle bin- and real-time monitoring of additional devices attached to a given host, etc.
The results show that these tools are completely appropriate for a large virtual infrastructure with critical devices. This platform completely ensures the constant monitoring, the timely notification of all responsible users when a problem occurs and it overcomes the problem using of external user's scripts.

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
(Aleksieva V., I.Zhelyazkov, Study of DoS attacks, UNITECH’16,18-19 November 2016, GABROVO – vol. II, p.162-167, ISSN 1313-230X)

This paper presents an investigation of network DoS attacks, using protocols of TCP / IP suite - UDP, TCP and ICMP. It is made in a laboratory network, using a developed system by authors in previous research for generation of DoS attacks. The purpose of the investigation with developed system is to offer versatile tools for simulating different types of attacks and to measure the harm of them. DoS attacks with various parameters are implemented.
The tests were performed on a local Ethernet or WiFi network:
1. Ethernet load test for DoS attack
The purpose is to monitor the state of the system of the attacked machine during a continuous DoS attack. In the first tests the parameters of the attacked machine are: CPU Intel Core2Duo T7700 2x2.40 GHz; RAM (physical) 2.00GB ddr2; OS Slackware 32-bit. The parameters of the attacking machine are: CPU Intel Core i7 vPro 4x2.13 GHz, RAM (physical) 4.00GB ddr3; OS Kali Linux 2.0 sana 64-bit. The test performed is only with a prolonged ICMP attack on the attacked machine. The attack machine launches 100 threads, simulating an attack from 100 different sources. As a result of the attack, the CPU load of the attacked machine increases by more than 50%. Other attacks were carried out similarly. In the first tests, there was a drastic jump in CPU load after the start of an ICMP attack, as well as when performing other types of attacks. An exception is the SYN flood attack, which generates a large amount of incoming traffic to the attacked machine. As a result of the ICMP attack, the attacked machine fails to respond in time to various user actions. The purpose of the second group of tests is to attack a more powerful machine than the previous one and to monitor the effect on the system during each attack in an Ethernet environment. The parameters of the attacked machine are: Windows 10 Pro; CPU Intel Core i5 430M 4x2.27 (4 logical cores); RAM (physical) 4.00GB ddr2. The parameters of the attacking machine are: Kali Linux 2.0 sana 64-bit, CPU Intel Core i7 vPro 4x2.13 GHz, RAM (physical) 4.00GB ddr3. In the second load tests, where a machine with a quad-core processor is attacked, 500 threads are executed in parallel for each attack (ie it implements 500 separate attacks). The load to which the attacked machine is subjected is significantly less (by up to 30% less) than the load observed in the first group of tests.
2. WiFi network load test in case of DoS attack
The purpose of this group of tests is to track the effect on the system of the attacked machine during each attack on a WiFi network. The parameters of the attacked machine are as in the previous tests. Due to the higher bandwidth of the copper cable at the same time, the incoming traffic to the attacked machine is significantly less than that arriving when transmitting data over a wireless network, which also affects the CPU load. The small amount of data does not force the operating system of the attacked machine to use the CPU in reduced capacity.

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

Vibrations have become an important factor of vehicles. Vibration tests help identify, and then tune the automotive vehicle to improve the structural strength. Vibration testing is often carried out using Laser Doppler Vibrometry (LDV), a device that is used for contactless measurement of vibration on the surface. The laser beam is directed from the device to the surface of interest, and the amplitude and frequency of vibration are extracted from the Doppler shift frequency of the reflected laser beam due to the movement surface. High values of vibration transmitted from the engine, and the way significantly affect the body of the vehicle and the driver are investigated.
Article presents results of research carried out on vehicles powered by three different engines and rpm. Tests were carried out on an engine dynamometer in the same environmental conditions. Two of engines were with spark ignition, including one with a supercharged engine and compression ignition engine.
The measurements were made using the Laser Doppler Vibrometry using Fast Fourier Transform. The spectrum obtained is used for further analysis to determine the acceleration level at various frequencies. Obtained from Fast Fourier Transform readings used for drawing graphs of frequency V acceleration.
As the rotational speed of the crankshaft increases (and the length of the period decreases), additional fluctuations occur in all types of vehicles (they were clearly seen even for the lowest velocity of the supercharged engine), but the vibration signal is of stationary character.
The diagrams show unambiguously that the amplitude of the relative vibration velocity notwithstanding the measurement target is the greatest for the vehicle with compression ignition engine and the lowest for the vehicle with spark ignition engine (non-supercharged). Simultaneously, the fluctuations and mean values of the signals indicate that the vehicle with diesel engine that is most ergonomic, whereas the vehicle with supercharged spark ignition engine is least ergonomic.

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
(Mitev Z., S.Valchanova, V.Aleksieva, Custom monitoring and management of virtual infrastructures based on Zabbix, Best Paper, 55th Science Conference of Ruse University, Русе, 28-29.10.2016, University of Ruse Publishing Center, p.229-234, ISSN 1311-3321)

This paper proposes a solution that implements several scripts for full and high-quality monitoring of virtual infrastructures - for monitoring websites, filling in information about the host (client), monitoring processes in Windows services, sending notifications to Gmail clients, monitoring Apache server, monitoring the size of the Recycle bin in real time, monitoring additional devices attached to a host.
Zabbix can use a low-level search rule to automatically detect VMware hypervisors and virtual machines. The default Zabbix dataset provides several ready-to-use VMware vCenter and vSphere monitoring templates. These templates contain preconfigured rules, as well as a number of built-in checks for monitoring virtual installations. In addition to the built-in checks in Zabbix, it is possible to create and customize checks. The Zabbix agent also has the ability to execute custom scripts. Thus, its functionality can be increased according to the personal needs of the respective virtual infrastructure by creating scripts written in Shell script, Perl, Python, Ruby, etc.
A Linux server with OpenSuse v.13.1 distribution and a test machine with Windows Server 2008 were used for test implementation of the system. Both machines are virtual and run on VMWare ESX server. Zabbix server, Zabbix agent, Zabbix frontend, Postfix mail server, MySQL database, Apache server, SNMP server, Web browser without graphical interface and text editor are installed on the Linux server. A Windows Server SNMP server is installed and the Zabbix agent is configured to send messages to the Zabbix server address.
For the purposes of experimental research to implement monitoring and management of a virtual structure with critical components, the following scripts have been developed:
1. Automatic entry of host information in the Zabbix frontend
2. Monitoring processes such as ping to host, CPU usage level, Apache server operation and notifications
3. Monitor the operation of processes in Windows Services
4. Real-time website monitoring
5. Keeping an audit log
The obtained results prove that the use of Zabbix is most suitable for large infrastructures with critical devices. This platform categorically guarantees constant monitoring, timely notification of all responsible users in case of a problem, as well as its elimination through the use of external user scripts.

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 is a wireless technology, which provides low power consumption of devices in personal area network (WPAN) for low data rate applications that require long battery life and secure networking. ZigBee gives effective ways of supporting of QoS (Quality of Service), functionality and manageability, because ZigBee devices can transmit data over long distances (more than 100 meters) by passing data through a mesh network of intermediate devices to reach more distant ones.
In this paper is proposed a simulation framework for ZigBee technology. It implements modified algorithm for the construction of a priority-based and energy-balanced WPAN network and visualize the method of transmission.
One approach to solving the problem of direct collision is Time-Division approach. Another approach is the Beacon-Only Period. Proposal to solve the problem of indirect collision is Reactive method. In this method each device (router or end device) must have the ability to transmit time information for beacon frames from its parent to its neighbors. This approach is complicated for sorting table from neighbor coordinators, because they need frequent updates, but it eliminates the possibility of developing an indirect collision.

The current approach offers a modification of algorithm proposed in previous author research. The basis of the proposed algorithm stands method of pricing based on which builds effective energy-balanced prioritized tree structure of ZigBee devices.
In this method it is assumed that routers only serve to build the topology and do not work as end devices.
In this modified algorithm first connect routers in the network tree to be able to build a network, then the end devices connect to them. When connecting router to router, or router to the coordinator, the cost of the parent does not change. In the case when the device is with a sufficient current paying ability, it is connected to the router who has the smallest number of children.
This algorithm changes the topology without priorities to the better topology, where devices work with low energy consumption.
The results of the conducted experiments are given. It used the simulator, created by authors in another research. To infer the number of collisions occurred it is monitored average speed of transmission of packets of varying lengths of transmission via ZigBee network created by the classical method and the method of pricing. In both cases the ZigBee network consists from the same devices with the same volumes of transmitted data. There has been improvement in the average rate of transmission in network topology achieved with the proposed algorithm of pricing.

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

This article presents an expanded and supplemented version of Г8.1, where is presented a system for generation of network DoS attacks, using protocols of TCP / IP suite - UDP, TCP and ICMP. The purpose of the developed system is for education and it offers versatile tools for simulating different types of attacks. DoS attacks with various parameters are implemented.

For realization of the proposed generator of DoS attacks is selected operation system - Kali Linux 2.0 sana, because it is optimized for performing penetration tests and many of the restrictions imposed by other popular Linux distributions and in most versions of Windows (except Windows XP / 2000 / Server 2000/2008), with respect to the RAW socket, are absent. The selected programming environment is Code Blocks 10.05, with the compiler GNU GCC.

The proposed generator of DoS attacks provides the following features:

- set of popular DoS attacks to perform simulation tests;
- set of tools for customizing the parameters of the attack;
- tools for automated tests in order to re-simulation of various scenarios with minimal user intervention;
- good performance and high level of control on the performed tests;
- low system requirements;
- simple and intuitive set of commands;
- creation of log files for analysis.

The results of tests for each kind of network attacks (UDP/ TCP flood attack, ICMP flood attack, SYN flood attack) are presented. Tests are provided in two similar experimental situations - the attacked machine at the first situation is running under Linux Slackware, and at the second - under Windows 7. Tests are provided in the local Ethernet network.

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

In this paper is proposed a simulation framework for LTE technology, which realized a priority-based algorithm for LTE Scheduler, which reorders packets, based on classification mechanism.

The aim of the proposed algorithm is to achieve keeping the network throughput as high as possible at a small price of only a bit more handovers. The functions for management of QoS in access networks are responsible for the efficient allocation of resources in a wireless interface. They are generally defined as the control algorithms of radio resources and incorporate power management, control of the transfer connection, access control, load control and the management packet, but directly related to QoS level cell are the last three. They are used to ensure a maximum throughput for individual services.

The present paper offers an algorithm for UEs service in the distribution of resources in the uplink of LTE network as composed of two modules - by a control mechanism for admission (admission control) and Scheduler. According to the network load, the admission control for the reception of orders manages the number of UEs, which can enter into the Scheduler, in order to avoid overloading the system with too many UEs.

The Scheduler allocates RBs among UEs according to UEs needs based on the priority.

A simulation environment was established for implementation and exploration of the proposed algorithm. Used software tool is Visual Basic 2010. On this stage of simulator, the data from different experiments are send in .xls format to the next estimation.

The results give reason to conclude that the presented algorithm for admission control in the Scheduler for LTE network can be applied successfully in the number of UEs under 100, because regardless of the intensity of the requests of the active UEs the average connection time is under 25ms-time, fully satisfying the requirements of 3GPP standard.

Simulation's results show that the proposed mechanism improves QoS, but the observed parameters degrade when the use of more subscribers is related to the priority implemented Scheduler, in which less priority queues may not be served in the case of network overload or congestion. There are presented drop ratio with prioritization and without prioritization. This algorithm always assures a minimum transmission for all the service classes, although with different performances due to prioritization.

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

This paper proposes an algorithm for resource allocation in an indoor LiFi network, which determines the priorities of the devices and allocates the resource blocks in a time slot between them based on this priority. A simulation environment has been created for its implementation, which allows visualization of the method of transmission between devices in LiFi infrastructure star topology network with two-way communication, in which the resource is shared between users in uplink direction based on an original algorithm for their prioritization.

The proposed algorithm allocates the resource blocks in a time slot by prioritizing the traffic by several parameters:

1. The first criterion is the distance to the access point, which is limited according to the range of each access point. The closer device has the higher priority. At equal distances, proceed to the next criterion.
2. The second criterion is whether the device is mobile or static. If it is mobile, the speed at which it moves must be entered. The simulation is for LiFi system indoors, so it cannot move more than 5 km/h (average speed per walking person). Mobile devices take precedence over stationary ones, but a device with a lower speed has a higher priority.
3. The third criterion is the types of services provided. Each access point may provide one or more types of services to a user. Each of these services belongs to a corresponding class, which has a different priority according to the QoS parameters. Handover Calls, Link Recovery Calls and Voice Calls belong to the class with the highest priority (Class1). Video Calls belongs to Class2, which is next in priority. Browsing, HDTV and Voice Messeges belong to Class 3, and the Background traffic belongs to the lowest priority class - Class4.

LiFi is a new technology on the market, extremely expensive compared to alternative solutions and with a small number of commercial conversions. Currently, there are no simulation environments to study the parameters of LiFi technology related to QoS improvement. This requires the development of own solutions for research and testing of approaches to solving emerging problems in possible implementations of LiFi. A simulation environment has been created for the implementation and research of the algorithm proposed in the present study. The software used is Visual Basic 2010. A database has been created to store the data from the individual experiments for the access points and the devices connected to them. In order to ensure the universality of the created simulator and due to the fact that there is no uniformly approved translation of the terminology related to LiFi, the language English was chosen for the implementation of the simulator.

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

This article is an expanded and supplemented version of the paper Г8.10. In this paper is proposed a simulation framework for LTE technology, which realized a priority based algorithm for LTE Scheduler, which reorders packets, based on classification mechanism.

LTE uses multiple access technology (OFDMA), where the total bandwidth is divided into Resource Blocks (RBs) in the frequency domain. The Data is transmitted in the Transport Blocks (TB) in one transmission time interval (TTI) for 1ms. Each RB consists from 12 subcarriers (each of them is 15kHz). The frame is 10ms and divides into 10 equal subframes. Each subframe contains 2 slots*0.5ms. Each RB is related to one slot in time. One TB is related to 1 subframe and it is the minimum unit to schedule. The serve rule is to find first space that can fit the TB. If there are not enough RBs in the current TTI, the scheduler tries to find resources in the next TTI. This strategy minimizes the response latency, which is the best practice for delay sensitive traffic. But this procedure is not applicable for beacon transmissions (it is sent among devices each 100ms), because of emergency information it conveys, therefore the reserved resource blocks exist to accommodate the temporary overload.

The present paper offers an algorithm for UEs service in the distribution of resources in the uplink of LTE network as composed of two modules - by a control mechanism for admission (admission control) and Scheduler. According to the network load, the admission control for the reception of orders manages the number of UEs, which can enter into the Scheduler, in order to avoid overloading the system with too many UEs.

The Scheduler allocates RBs among UEs according to UEs needs. Resource allocation in the Scheduler is based on the priority of the traffic (highest is the first):

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

A simulation environment was established for implementation and exploration of the proposed algorithm. It has modular architecture. The input of data for each device starts from initial parameters for the 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

This paper presents tools for testing of vulnerabilities in wireless networks, based on the techniques "man-in-the-middle" and social engineering. It works under Kali Linux with multi-language interface. The tool gives the possibility to check the level of password protection for WiFi Networks with different encryption, such as WEP, WPA and WPA2. The development is modular and it allows to be extended easily. The results from experimental research are presented.

The present development uses the active method to investigate the security of wireless networks and presents a vulnerability investigation tool developed under Kali Linux. The tests of wireless networks conducted and presented here are for educational purposes and are made in laboratory environment. An operating system - Kali Linux 2.0 sana was chosen for the implementation of the attack generator. It is optimized for performing penetration tests and a number of restrictions imposed in other popular Linux distributions and in most versions of Windows (except Windows XP / 2000 / Server 2000/2008), in terms of RAW sockets, are absent. Kali Linux is now officially available for smartphones such as Nexus 5, Nexus 6, Nexus 7, Nexus 9, Nexus 10, OnePlus One, and some Samsung Galaxy models, which makes it possible to install the application on a mobile device.

The necessary modules for the proper operation of the application are: Aircrack-ng, Aireplay-ng, Airmon-ng, Airodump-ng, Awk, Curl, Macchanger, Mdk3, Nmap, Pyrit and others. If any of them is not installed, the application notifies you of the required installation and stops working.

With the presented application for testing the stability of the wireless networks, the wireless routers for retrieving their passwords have been attacked. Several types of attacks were performed, each measuring the time for which full access to the attacked wireless network was achieved.

The proposed solution can help to improve and test the security of any wireless network, but also to allow for tests and simulations in real time, as close as possible to the real environment where the network will operate in critical conditions.

This report also presents the results of experiments that prove the effectiveness of the proposed software tool for investigating security vulnerabilities in wireless networks. Its modular implementation allows in the future to implement other types of popular attacks, which are not aimed only at wireless networks.

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

In this paper is proposed a web-based management system for AD, which provided a seamless and simple experience to the IT administrators and synchronize directories between on-premises to the cloud, and by doing that the same identity is used on both environments.

The developed Web-based system (MATEX) manages ADs. The server side is based on PowerShell skripts and cmdlets. The system has developed with Visual Studio 2010, ASP.NET, C#, and Windows Powershell.

The MATEX has worked on three virtual machines (VM) - two servers (BGVARNADC01, JPTOKYODC01) and one client USTESTPC01. On the first server BGVARNADC01 (Windows Server 2012R2 Std) / VM have started AD Primary Domain Controller (PDC) and all FSMO roles holder, DHCP Primary server, ISS Web server, File server, SMTP server, Backup server. On the second server JPTOKYODC01 (Windows Server 2012R2 Std)/ VM have started AD Domain Controller server, DHCP backup server, WSUS server, File Server, Backup Server. The third VM USTESTPC01 (Windows 7 Pro)/VM has role of client workstation and there have configured Dynamic DNS record to joined into the domain and IP settings from DHCP server.

The Matex.com domain is made up of two domain controllers (DCs) - BGVARNADC01 and JPTOKYODC01, which a bidirectionally replicate all AD containers and DNS containers. Thus, a change or action done on one DC is replicated and is visible to the other. The default replication time is one hour.

The Organization Unit (OU) structure is divided into 3 levels for easier management and classification of users and resources (Region Level - Africa, Asia, Europe ...; Country Level - China, India, Japan ..;Site Level - Fuji, Kobe, Tokyo ....).

The DNS functionality in MATEX is integrated into the Active Directory as dynamic sign-up allowed only for domain customers. This fact does not allow personal computers from outside the domain to be registered. Aging / Scavenging functionality is set, and both options are 7 days. This means, that dynamic DNS record will be automatically deleted after 14 days if the client machine is inactive during this time.

To determine the performance of the MATEX are applied various tests, by simulating employability for a certain number of users, who use the site at the same time. The MATEX manages simultaneous queries of 5, 10 and 15 users simultaneously at the same time. In case of 20 simultaneously active users, there are already observed moments where productivity falls significantly at certain times.

The average time of multiple "clicks" was measured for a different number of users (5,10,15) made at the same time. It is very small. For 20 users, the average time doubled. The conclusion is that 20 is the limit of both active users who use the MATEX, because over this number the productivity and performance slow down.

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

This paper presents a research if there is a relation between the user pose (standing, sitting or lying) and the position of two-finger touches on the wearable device bezel caused by the user hands posture differences. Finding and proving such relation will open many opportunities for improving computer-human interfaces of the wearable devices and the user experience. It could give the possibility for the devices itself "to learn" (via Machine learning methods) user behaviors not based only on the time when the interface is activated but also counting on the user pose. Applying such algorithms could push the device interface not to follow the pre-ordered and coded into the device OS or software menus' flow but to start with the applications or the device settings which are typical for the user based on user pose recognition. It will reduce the device interaction time and the user efforts to complete the needed device input tasks. Knowing in which pose is the user and the day time it could be managed also the device display brightness, interface colours, icon style, etc. in order to provide better user experience and save the device energy.

The experimental data shows that for any two given poses (from all three possible poses) it would be possible based on the position of the users' fingers over touch sensitive bezel of a wearable device (smartwatch) to:

- differentiate between standing and sitting poses (Dsc) with 60% probability
- differentiate between sitting and lying poses (Dcb) with 80% probability
- differentiate between standing and lying poses (Dsb) with 90% probability

The conclusion is that the lying pose could be differentiated with higher enough probability while the sitting and standing poses in more than half of the cases (60%). If we base the pose recognition method on the relative "deltas" we could achieve even highest probability.

The presented method is not related to the leading user hand (with which the user operates with its device) so the described methodology can be applied also to users who wear the device on their right hand (respectively control the device with their left hand).

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
(Aleksieva V., V.Dimitrov, Desktop application for training in data coding and modulation visualizations, //Computer science and tehnologies, TU-Varna, 2018,No1,p.39-45,ISSN 1312-3335)

The proposed desktop application realized most popular lossless data compression algorithms. In addition, it visualizes coded strings with the basic modulations. The idea is to present the same message text in different code scheme and see how they looks as modulated string in the network media. This application is completely useful in labs on subjects, related to network communications.
Microsoft Visual Studio 2012 environment and C # programming language are chosen for the presented desktop application for data encoding and modulation visualization.
The functional requirements for the application are:
• to allow the user to enter their information (a series of ASCII symbols or numbers) and based on it to visualize the selected modulation - amplitude, frequency, phase;
• to allow the user to enter their information, and based on it to demonstrate its coding by different algorithms - parity code, cyclic code, Heming code and Shannon-Fano code;
• to allow the user to check and detect with the application errors of already encoded information.
The non-functional requirements are:
• the interface of the application to be in English language in order to allow it to be used in the training course in both Bulgarian and English
• simple and intuitive interface
• automatic visualization of modulations and coding results.
In view of the target group for which the application is intended and according to the course in the “Basics of communications”, where it is used, standard implementation algorithms are selected, and the main types of modulations are provided for implementation - amplitude, frequency and phase modulation, such as phase modulation has a phase of 180^{o}. For the implementation of coding of symbols represented by ASCII code in binary form and numbers converted into binary number system, are chosen parity code, matrix parity code, cyclic code with 5 different polynomials, code of Heming and Shannon-Fano code.
At the moment it is applied in the course "Basic of Communications" in the Bachelor's degree in the specialty "Computer Systems and Technologies" both in the teaching of Bulgarian and in the teaching of English.

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
(Aleksieva V., A.Huliyan, Crypto-token based on a smart contract of Ethereum blockchain, John Atanasoff Society of Automatics and Informatics, Sofia, October 4-6, 2018, ISSN 1313-1869, p.125-128

This solution is based on Ethereum because it allows the creation of smart contracts and the construction of applications that run on the blockchain itself. The smart contract certifies that participant “A” must pay a certain amount from his account to participant “B”, who will provide certain services to participant “A”. It is uploaded to the currency blockchain and a copy of it is available to every user of the system, so the contract is confirmed by the thousands of miners in it. Smart contracts are described through a new programming language created for this purpose - Solidity. On 11.09.2017, Ethereum adopted the standard for smart contracts EIP20 (Ethereum Improvement Proposal 20), compatible with all Ethereum portfolios and platforms. ERC20 describes variable names, functions and their functionality.
Based on smart contracts, Etherium provides the ability to build applications and fully integrate them into the blockchain - dApps (Distributed Applications). These applications are also signed with the electronic signatures of the users and only the holders of the private key can unlock the information that is there. GAS is used to run these applications, as well as code execution. In this way, developers are stimulated to create optimal code and prevent endless loops.
This solution was developed with Truffle and Ganache under the macOS High Sierra operating system. Truffle offers an integrated system for compiling written smart contracts, as well as scripts for uploading the contract to the Ethereum network. Ganache creates a local blockchain based on Ethereum, in which commands can be executed directly, as well as tests can be performed. The implementation of Ethereum blockchain is written in JavaScript.
In order to create a token, it is necessary to describe what its maximum quantity is, to create a way to check its availability, as well as functions controlling its transfer from one address to another. This is done through the proposed smart contract. The constructor initializes the maximum number of tokens and they are assigned to the address from which the constructor was executed. It is executed only once by the address that broadcasts it on the network. Events are used to store information in the transaction. Once recorded, this information will exist as long as the block in which the transaction is located is visible. With the current implementation of Ethereum, that means forever. The recorded information is not available from smart contracts, even from the one who created it. Their main application is when using user-defined JavaScript functions that wait for a certain event to occur in order to perform an action. In this implementation, the "Transfer" event reflects the movement of tokens from one address to another, as well as their number, and "Approval" performs a similar action, but gives permission from the owner of the tokens to be spent by someone else.
The proposed smart contract has been tested with the built-in Truffle testing mechanisms and the results show that it is fully functional.

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
(Aleksieva V., A.Huliyan, Etherium blockchain smart contract, UNITECH’18,16-17 November 2018, GABROVO, vol.II, pp. 117-122, ISSN 1313-230X)

Nowadays smart contracts allow to perform credible, trackable and irreversible transactions without third parties. There are some possible applications of smart contracts, i.e. in logistics, management, bank system, insurance, estate, IoT, and others. The proposed paper presents the implementation of a smart contract based on Ethereum blockchain. The decentralized crypto-token is created for Initial Coin Offering (ICO) and based on the ERC20 standard. A web-based interface is created for the sale of these crypto-tokens. The results from the experimental tests are presented.
The proposed solution was developed with Truffle and Ganache under the macOS High Sierra operating system. The application fully complies with the EIP20 standard and uses the specialized programming language for smart contracts Solidity. The application interface uses web3.js (a JavaScript-based library that allows to communicate with the Ethereum network and execute smart contracts). The client side of the application requires the use of an add-on to an existing Metamask browser.
In order to create a token, it is necessary to describe what its maximum quantity is, to create a way to check its availability, as well as functions controlling its transfer from one address to another. This is done through a smart contract implementing the ERC20 standard, called by the authors AutoCoin. An already uploaded smart contract cannot be deleted or changed, but a new version is uploaded. Variables for the number of tokens sold, price per token and the administrator of the smart contract for the sale of tokens are declared as global. The price for one token is 0.01 Ethers for a token.
The interface of the application provides information about the number of tokens for sale, the number of purchased tokens, information about the address to which the user has contacted him, as well as the available number of tokens. Enter the amount of Ethers to be transferred, the transaction fees, the maximum GAS that can be spent during the transaction, and it is possible to manually enter the price for GAS presented in GWEI. This price directly affects when the transaction will enter the block. At a price of 40 GWEI is almost completely guaranteed entry into the next block, 20 GWEI usually means inclusion in the next few blocks, with a minimum amount of 2 GWEI sometimes it takes a few minutes to enter a block. If a low value is set and the transaction does not enter a block, it is possible to adjust the price to a higher one, for faster execution of the transaction.
Experimental tests are presented, which prove the operability of the proposed smart contract for ICO and its manageability through the proposed web-based interface.

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

This article presents an extended version of the paper Г8.14.
Active Directory (AD) is the one of the last categories to make the transition to the cloud. AD as SaaS will give solution to the IT administrators can take advantage of the synchronized directories between on-premises to the cloud, and by doing that the same identity will be used on both environments.
In this paper is proposed a web-based management system for AD, which provided a seamless and simple experience to the IT administrators and synchronize directories between on-premises to the cloud, and by doing that the same identity is used on both environments.
The developed Web-based system (MATEX) manages ADs. The server side is based on PowerShell skripts and cmdlets. The system has developed with Visual Studio 2010, ASP.NET, C#, and Windows Powershell.
To determine the performance of the MATEX are applied various tests, by simulating employability for a certain number of users, who use the site at the same time.
The MATEX manages simultaneous queries of 5, 10 and 15 users simultaneously at the same time. In case of 20 simultaneously active users, there are already observed moments where productivity falls significantly at certain times.
All web pages and scripts from the MATEX load for approximately the same amount of time for multiple user queries.
The average time of multiple "clicks" was measured for a different number of users (5,10,15) made at the same time, which is very small. For 20 users, the average time doubled. The conclusion is that 20 is the limit of both active users who use the MATEX, because over this number the productivity and performance slow down.

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

The proposed paper presents a solution for the creation of a decentralized token for the implementation of a smart contract based on Ethereum block-chain. A web based interface has been created for Initial Coin Offering (ICO). In the experimental environment the research was carried out for various scenarios. The results are presented.

This smart contract and web-based interfaces are presented in Г8.17 and Г8.18. In this paper are presented experimental tests and results for its functionality.

First part of the tests is related to the proper work of smart contracts- balance of account, transfer of tokens etc. There are a handful of tools for automated smart contract (written in Solidity) security vulnerability testing based on code-level analysis. In Reza's approach is given a synopsis of the four most related tools that is possible to use in experiments, namely Oyente, Mythril, Securify, and SmartCheck. However, the evaluate level of rigor, ranging from syntactic, heuristic, analytic to fully formal, refers to underlying security testing technique of the given tool and up to this moment the researchers trusted on the implemented in the Solidity test tools. Truffle (and Solidity) has a built-in smart-contract-testing mechanism that is written in JavaScript, which here is used.

For direct transfer testing, 250 000 tokens are transferred from the administrator's address to the recipient's address. Once the transfer has taken place, the event is captured and checked for "Transfer" type. If this test is successful, the balance of the recipient address is checked for the presence of transferred tokens.

The delegated transfer check is similar to the direct transfer check. First, 100 tokens are transferred from the administrator's address to the address from which a delegated transfer will be allowed - address 1. It is allowed 10 tokens to be spent from address 3, which sends them to address 4. After performing these actions, it is expected that address 1 to have 90 tokens, address 2 - 0, and address 3 to be 10 tokens. The result of their implementation with wrong and correct parameters are shown.

In the real Ethereum block, as much as power to include block time is fixed, there comes a dynamic change of difficulty depending on how much power is included in the network. The tests were carried out in the local network with flat topology. The client connects to the Metamask server. The parameters of computers are Apple Mac Book Pro Late 2011 Specs, Core i5 (I5-2435M) 2.4GHz 2/4 Cores/Threads, 4GB DDR3 1333Mhz RAM. In the Metamask when sending an ether to buy a token, there is used protocol TLSv1.2. In the paper is presented network communication between client and Metamask server during successful transaction of tokens.

Г.8.21. Алексиева В., 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
(Aleksieva V., H.Valchanov,A.Huliyan, Application of smart contracts based on Ethereum blockchain for the purposes of insurance services, Informatics and inovative technologies, pp.7-14, No1(1),2019, ISSN 2682-9517)

This article presents an experimental implementation of smart contract for insurance service on the Ethereum blockchain. The authors present a classic model of insurance service and point out its shortcomings. On this basis, they offer a model for insurance services based on blockchain technologies. An experimental implementation on Ethereum blockchain is presented.
The claim processing process can be improved using smart contracts and blockchain technology. The information about the occurred damage can be sent by the insured or directly by sensors installed in the insured object (smart asset), to an automated application for processing a claim. For the relevant insurance policies provided by the smart contract, the customer will receive real-time feedback. The claim is processed automatically by a smart contract based on a set business logic, using information provided by the insured. DLT automatically uses additional sources (statistics, reports) to assess the claim and calculate the damage. Depending on the insurance policy, the smart contract can automatically calculate personal liability. In certain situations, a smart contract may activate an additional assessment of the claim. If the claim is approved, the payment to the insured is initiated through a smart contract.
The advantages of the new approach, based on smart contracts on blockchain technology, can be considered in several aspects. The submission of the claim is simplified and automated. Thanks to the direct exchange of damage information between insurers, DLT eliminates the need of brokers to participate and reduces the time for processing the claim. The built-in business logic in the smart contract in the blockchain eliminates the need for experts to review every claim (except in specific situations). The insurer has access to the history of the origin of the damage, which helps to identify potential attempted fraud. The information used is integrated, thanks to DLT's ability to aggregate data from multiple trusted sources. The process of paying the damage is automated by the smart contract on the blockchain, without the need to use an intermediary.
There are presented the advantages and the disadvantages of using private and public blockchain, as well as combined solutions with 2 blockchains (for automation of back-office operations to use a private blockchain, and for management of automatic payments with existing cryptocurrencies or when necessary to provide trust to use a public blockchain).
The presented solution is on the public blockchain Ethereum.

Г.8.22. В.Алексиева, Х.Вълчанов, Ю.Димитров, Изследване на интерфейси за смарт часовници, UNITECH’19,15-16 November 2019, GABROVO, vol.II, pp. 12-16, ISSN 1313-230X
(Aleksieva V.,H.Valchanov, Y.Dimitrov, Study of smart watch interfaces, UNITECH’19,15-16 November 2019, GABROVO, vol.II, pp. 12-16, ISSN 1313-230X)

Smart watches are wearable devices’ small sizes. Their display size and limited space for input controls require specific attention to the device interfaces development processes. The research in this paper aims to compare two different approaches in the interface design - a Novel interface based on two-finger touch interface activation and management on touch sensitive device bezel (the surface that is around the display) to a Standard “wristwatch” style input interface based on side push buttons.
The purpose of this study is to compare the process of human-smartwatch interaction, when the same user performs the same task using two prototypes of smartwatches developed for this purpose. For the purposes of the study, two experimental prototypes with different input interfaces were made - "Novel" with a touch-sensitive bezel interface, which was developed for a previous study, and "Standard" with four buttons on the side of the device, which is designed and developed for the current research.
In order for the research results to be completely comparable, the two models are made on the basis of the same 3D model of a wristwatch. The experimental models are controlled by a computer Arduino Mega 2560. Software has been developed to control each model based on Arduino. Both software products recognize four main interoperability command interfaces - Up, Down, Select, and Back.
The test group consists of 10 volunteers using their right hand to work with the prototypes. The average age of the participants in the experiments was 37.6 years. All experiments were performed under equal other conditions - in the same room, without artificial lighting.
The study of the developed models of smartwatch interfaces was conducted in three stages - the first stage compares the time and accuracy of a simple task (choice of only one function), the second stage compares the time and accuracy of a complex task (choice of function in several steps), and in the third stage the volunteers give a subjective assessment of the comfort of working with both interfaces.
Experimental data are presented.
The conclusions of the study can be summarized in the following:
• The new experimental model surpasses the standard in speed of work. When the set of commands is longer, the benefit of using the new interface model is greater.
• The error rates when working with the new model are higher than when using the standard model. The reason may be the fact that the traditional interfaces with side buttons on an electronic watch are familiar to most people, but the interface of the new model with a touch-sensitive ring is something new for them.
• Users' assessment of the comfort of working with both interfaces is higher for working with a standard model.

Г.8.23. Х.Вълчанов, В.Алексиева, Ж. Едикян, Изследване на сигурността в безжични мрежи, UNITECH'19, 15-16 November 2019, GABROVO, vol.II, pp. 7-11, ISSN 1313-230X
(Valchanov H.,V.Aleksieva,Z.Edikyan, Study of wireless networks security, UNITECH'19, 15-16 November 2019, GABROVO, vol.II, pp. 7-11, ISSN 1313-230X)

Wireless network allows easy to build small enterprise and home networks based on IEEE 802.11 standard. However, wireless networks are easily susceptible to attacks against their security. This requires an analysis of the problems and creating recommendations to improve their security. This paper presents a methodology and study of wireless network security in Varna city. The information was collected using the war-driving technique. The obtained results are analyzed and compared with those from previous studies.

The data collection system is based on a single-board computer Raspberry Pi 3 Model B, with ARM Cortex-A53 processor, 1.2GHz, built-in Wi-Fi and Bluetooth functionality. For the purpose of the implementation, it is necessary to record the position of each wireless access point. The chosen GPS module, due to support for the NMEA 0183 standard, long-lasting battery and large memory, is the Holux M-1200E. The CanaKit Wi-Fi Module is used to scan wireless networks. A Canyon CNS-TPBP5DG portable battery with a capacity of 5000mAh is used to provide a long-term power to the single-board computer.

The scan of the wireless networks is done using open source software Kismet. The software is compiled and installed under the Raspbian OS operating system. The data received from Kismet is saved in netxml format. The collected information is converted via Python script to csv format. This is necessary so that the data can be presented in tabular form for easier processing and analysis through Microsoft Excel. The selected area for analysis includes the central part of Varna, as it is home to most of the offices and most of the residents. Also, the region coincides with a similar study conducted in 2008, in order to compare the results obtained.

The results show a significant increase in the security of Wi-Fi networks in the city, but there is still room for improvement.

The reasons for improving security can be considered in two ways. First, manufacturers offer devices that have WPA2 configured by default. Second, larger organizations have IT departments that take care of security. Based on the results of the detected SSIDs, mixed mode WPA / WPA2 and WPS, it can be concluded that most of the analyzed Wi Fi networks belong to ordinary users who do not have sufficient security knowledge.

The main recommendations can be presented in the following areas:

1. Use only WPA2 encryption method.
2. Disable WPS for all devices.
3. Choose a complex password.
4. Update the device software to the latest version.
5. Inform users about Wi-Fi security issues.

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

In this paper is presented a simulation framework for realization of mobility in LoRaWan networks. Some of the many requirements of IoT conception are met in Low Power Wide Area Networks (LPWANs) - low cost, energy efficiency and large area coverage. One of the most studied implementation of LPWAN technologies is Long Range Wide Area Networks (LoRaWan). LoRaWan is a relatively new technology with many advantages and disadvantages. Some disadvantages can be fixed by studying the technology limits and making simulation frameworks through which to continue the further development of technology. In this paper is proposed a simulation system for the implementation of the Handover in LoRaWan, which realizes the end devices mobility and finding the best route between end devices after before and after, has been done. The implemented algorithms for finding the best route between end devices and simulating mobility are used to study and improve QoS parameters in LoRaWan networks.

The mobility (handover) in wireless networks can be caused by many reasons like physical movement of the connected device, changing network characteristics, etc. There are two different types of handover depending on what kind of access network each PoA belongs - Horizontal and Vertical handover.

The simulator performs the mobility in LoRaWan network based on the suggested mobility algorithm. The quality of the signal is checked for the realisation of mobility. The handover procedure start is based on the Received Signal Strength (RSS) value. A handover is provided when another gateway (terminal) with a higher RSS value is found. Mobility takes place in three stages, combining Layer 2 and Layer 3 handover.

The simulation environment has 6 blocks: GUI (Graphical user interface) – includes easy to use user interface for simulations ; Core – main block performing all operations of the simulator; Creating topology – block for creating topology; Topology modification – block for modification of existing topologies; Finding best path between end devices – using "Depth First Search" and "Hassle Free Route Algorithms" a best route between end devices can be found; Handover - with the help of this block mobile end devices are transferred to the new terminal devices that meet these needs in each of their directions of movement.

The “Chart” button in the “handover” tab opens the window where the results from the performed simulations can be analysed. A chart showing information for end devices - their type (mobile, static) and status (enabled, disabled) for each terminal, also a chart visualizing the number of mobilities performed between terminal gateways. A chart is presented for the MSNs, summarizing and representing the number of movements for each mobile end device which has performed mobility etc.