

РЕЦЕНЗИЯ

от проф. д-н Петър Стоянов Апостолов

на дисертационен труд за присъждане на образователно-научна степен „Доктор“, научна специалност 5.3. Комуникационна и компютърна техника - Компютърни комплекси системи и мрежи

на тема: *Анализ и симулационно изследване на особеностите на локални мрежи*

Докторант: инж. Илиян Иванов

Научен ръководител: доц. д-н Иван Тренчев

1. Данни за докторанта

Инж. Илиян Иванов е роден в Благоевград през 1981 г. Придобива образование в областите на икономика и право. Подобно на много други млади хора е увлечен от съвременните комуникационни и компютърни технологии. В този си стремеж към надграждане на образованието си, в периода 2016 – 2018 г. завършва магистратура “Компютърни системи и технологии” в ЮЗУ Благоевград. Успоредно с това, завършва и CISCO академия. От 2016 г. Илиян Иванов работи като системен администратор в Информационен и комуникационен отдел на ЮЗУ – Благоевград. От 2020 г. е хоноруван асистент в катедра Комуникационна и компютърна техника и технологии в Технически факултет на ЮЗУ.

2. Актуалност на дисертационния труд

През последните десетилетия областта на техническите комуникации претърпя революционен скок. Основната задача в комуникациите е предаването на максимален обем информация с минимални ресурси като: технически средства, енергоемкост, изчислителна сложност и себестойност. Освен това, предадената информация трябва да бъде с минимален брой

грешки. В тези насоки се създават нови технологии, математически модели, технически средства и се очертават нови перспективи в развитието на тази научно-техническа област. Неделима част от комуникационната техника са компютърните мрежи. В този дух, описаните анализ и симулационни изследвания на локални компютърни мрежи в дисертационният труд на инж. Илиян Иванов са актуални и в съответствие със съвременните тенденции на развитие на комуникационната техника.

3. Обща характеристика на дисертационния труд

Дисертационният труд е разработен в три глави, увод и заключение с обем 193 страници стандартно оформен текст, включващ фигури, графики, таблици, формули и приложения. Библиографията включва 337 заглавия на английски език, включително и линкове към електронни издания.

Уводът е въвеждащ в областта на безжичните компютърни мрежи. Най-общо са описани предназначението, функциите и критериите за осигуряване на максимална скорост на предаване при минимално отношение на сгрешени към правилно приети битове - BER. Отбелязани са най-използваните безжични стандарти Bluetooth , IEEE 802.15.4/ ZigBee, WiFi (802.11*), Wi-Fi Direct. Формулирани са целите и задачите на дисертационния труд.

Първа глава представлява образователната част от дисертацията, която няма да коментирам подробно. В обобщен вид са изложени видовете компютърни мрежи, техните характеристики и параметри. С оглед на задачите на дисертационния труд, докторантът е наблегнал на безжичните мрежи: изграждане, комуникационни устройства, стандарти за безжично предаване на данни, топологии на безжичните мрежи, протоколи за множествен достъп, колизии при множествен достъп.

Изложението е извършено старателно с позоваване на много съвременни литературни източници.

На основата на изложението в образователната част, в *Глава втора „Методология и обзор“*, докторантът е приел за изследванията си перспективната технология за безжична връзка - стандартът IEEE 802.15.4/ - ZigBee. Обстоятелствено са изложени предимствата на стандарта – ниска енергоемкост, високо бързодействие при създаване на връзки, приложимост при различни видове топологии при голям брой възли. Описани са и интегрални схеми, които реализират този тип технология и е направен сравнителен анализ на параметрите им.

Докторантът е обърнал особено внимание на проблемите на сигурността на връзките. Разгледани са различни видове хакерски атаки за несанкциониран достъп до информация в мрежите, както и нарушаване тяхната функционалност.

В *Глава трета – цели и задачи* е направен анализ на предаването на данни в различни компютърни мрежи. Изтъкнати са предимствата на цифровото предаване на данни пред аналоговото предаване на данни. Пунктуално са посочени целите на изследването:

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

От поставените цели докторантът е формулирал следните задачи:

1. Концептуален анализ на методите и подходите за анализ на компютърни мрежи и софтуерни системи.
2. Преглед на различните видове протоколи и описание на техните различия – обзор по темата.
3. Разработване на различни софтуерни симулации като се използват различни протоколи и да се анализира преноса на данни и някои характеристики на компютърната мрежа като стабилност на данните, честотна лента и др.
4. Приложение на нова математически подходи за анализ и прогнозиране на стабилността на компютърна мрежи и информационната система в частност.
5. Тестване на компютърни симулации и реализиране на хакерска атака като се анализират различни начини на ентропия и сложността на проведената атака.

В частта *Дискусия* е под форма на литературен обзор са дебатирани методите и подходите за анализ на компютърни мрежи и софтуерни системи. С похвално старание докторантът се е позовал на внушителен брой литературни източници в областта на дисертационния труд.

Следва способ на хакерска атака към компютърна система с Raspberry PI по метода на грубата сила. Докторантът обстойно е описал как може да бъде „открадната“ паролата на WiFi мрежа със съответния хардуер и софтуер.

В съответствие с поставените цели, в дисертационния труд са демонстрирани компютърни симулации на различни протоколи със софтуерния пакет Matlab. Изтъкната е перспективността на системата MIMO-OFDM (Multiple-Input Multiplexing и Orthogonal Frequency Separation) за редуциране на нежеланите ефекти от интерференция на

радиовълните в урбанизирани среди. Представен е пример за създаване такава комуникация с 16-елементна линейна фазирана антенна решетка. Получените диаграми на насоченост са с пространствена селективност, която намалява интерференцията на сигналите. Използван е MUSIC (MUltiple SIgnal Classification) алгоритъм за определяне на пространствения спектър, посоката и закъснението на сигналите.

Изследванията продължават с многопортова пасивна мрежа, QoS (Quality of service) планиране на трафика, Модел 802.11ax на безжична връзка, кабелния интерфейс или DOCSIS.

Достойнство на дисертационния труд са представените резултати от тестване на компютърна система в реално време с програмен продукт Evolink.

Като допълнение към теорията са разгледани математически модели за анализ на компютърна система: Теория на игрите, Теория на катастрофите, Теория на масовото обслужване.

Особен интерес представляват таблиците със сравнителен анализ на хакерските атаки върху държавните структури на Република България.

В заключителната част авторът е изложил своите претенции за приноси както следва (цитирам):

1. Открити са проблемни области в областта на обмен на информацията при различни компютърни мрежи и е направен систематичен обзор.
2. Представени са различните методи хакерски атаки и методи на тяхната защита тази група атаки включва всеки опит за получаване на неоторизиран достъп до системата. Направен е анализ на различните видове атаки като:

- Атаки от тип „отказ от услуга“ (DoS): вид атака, която причинява загуба на услуга или невъзможност на мрежата да функционира.
 - Уеб атаки: това е всяка атака, която се опитва да наруши/промени даден уеб сайт. Две от най-често срещаните такива атаки са: SQL injection (SQLi).
 - “Отвличане” на HTTP сесии (Session hijacking): тези атаки представляват отвличане на идентификатора на потребителската сесия (session hijacking).
 - DNS отравяне (DNS poisoning): този тип атаки компрометират DNS сървърта така, че потребителите могат да бъдат пренасочени към зловредни уеб сайтове.
3. Разработен е метод на хакерска атака по метода на грубата сила. Реализиран с хибриден компютър от типа Ардуино. Направен е анализ на сложността на атаката.
 4. Разработени са математически модели за анализ на стабилността на сигурността на компютърна мрежа и начини за анали на тази система. Използвани са математически подходи като Марковски процеси, Теория на игрите с природата с приложение на принципа на Белман и Теория на катастрофите.
 5. В софтуерния пакет Матлаб са направени множество симулации за анализ на преноса на данни в различни компютърни мрежи и влиянието на шума върху този пренос.
 6. Анализирани са трафика на компютърна мрежа на интернет доставчик и са систематизирани основните атаки извършвани върху доставчика.
 7. Направен е концептуален анализ на видовете компютърни атаки и начините им на провеждане върху бюджетните предприятия.

По мое мнение изброените приноси са с приложен характер и претенциите на автора са основателни.

6. Забележки и препоръки

Имам следните забележки и препоръки.

Оформлението на дисертационния труд е необичайно и прави повествованието трудно за възприемане.

В началото на дисертацията липсва литературен обзор. Донякъде точката „Дискусия“ има характер на такъв обзор.

В голяма част от дисертацията са ползвани източници на английски език и преводът е неясен и с объркан словоред. Някои специфични технически термини са преведени с български синоними, които са неточни.

Математическите методи са представени доста безразборно. В аналитичните изрази няма обяснение за параметрите в тях, което ги прави малко „откъснати“ от общото изложение в дисертацията.

Бих препоръчал на инж. Илиян Иванов да се ориентира към усъвършенстване на способностите си в областта на компютърните мрежи.

7. Публикации

В материалите към дисертационния труд инж. Илиян Иванов е представил списък с четири научни публикации, две от които в съавторство са публикувани в престижната библиотека от бази данни Web of Science. Това е една добра атестация за публикационната активност на инж. Илиян Иванов.

Заключение:

Предложената дисертация има качества, които се потвърждават от получените резултати. Предоставените ми материали са достатъчни за покриване на критериите и изискванията на НАЦИД. Това ми дава основание да предложа на Научното жури да присъди на инж. Илиян Иванов образователно-научната степен „Доктор” в област на висшето образование

5.3. Комуникационна и компютърна техника - Компютърни комплекси системи и мрежи.

Рецензент:.....

27. 02. 2022

/проф. д-р инж. Петър Апостолов/

REVIEW

by Prof. Peter Stoyanov Apostolov, ScD

of thesys for awarding the educational-scientific degree "PhD", scientific specialty 5.3. Communication and computer equipment - Computer systems and networks

on the topic: *Analysis and simulation research of the peculiarities of local networks*

PhD student: Eng. Ilian Ivanov

Scientific adviser: Assoc. Prof. Ivan Trenchev, ScD

1. Data for the doctoral student

Eng. Ilian Ivanov was born in Blagoevgrad in 1981. He received his education in the fields of economics and law. Like many other young people, he is fascinated by modern communication and computer technology. In this quest to upgrade his education, in the period 2016 - 2018 he completed a master's degree in "Computer Systems and Technologies" at South West University - Blagoevgrad. In parallel, he graduated from CISCO Academy. Since 2016, Ilian Ivanov has been working as a system administrator in the Information and Communication Department of SWU - Blagoevgrad. Since 2020 he has been a part-time assistant in the Department of Communication and Computer Engineering and Technology at the Technical Faculty of South West University - Blagoevgrad.

2. Relevance of the thesis

In recent decades, technical communications have undergone a revolution in their development. The main task in communications is the transmission of the

maximum information with minimal resources such as: technical means, energy consumption, computational complexity and cost. In addition, the information transmitted must have a minimum number of errors. In these directions new technologies, mathematical models, technical means are created and new perspectives in the development of this scientific and technical field are outlined. An integral part of communication technology are computer networks. In this spirit, the described analysis and simulation studies of local computer networks in the dissertation of Eng. Ilian Ivanov are relevant and in line with modern trends in communication technology.

3. General characteristics of the dissertation

The dissertation is written in three chapters, introduction and conclusion with a volume of 193 pages of standard text, including figures, graphs, tables, formulas and applications. The bibliography includes 337 titles in English, including links to electronic publications.

The introduction is introductory in the field of wireless computer networks. The purpose, functions and criteria for ensuring the maximum transmission speed with a minimum ratio of erroneous to correctly received bits - BER are generally described. The most used wireless standards are Bluetooth, IEEE 802.15.4 / ZigBee, WiFi (802.11 *), Wi-Fi Direct. The goals and tasks of the dissertation are formulated.

The first chapter is the educational part of the dissertation, which I will not comment on in detail. The types of computer networks, their characteristics and parameters are summarized. In view of the tasks of the dissertation, the doctoral student focused on wireless networks: construction, communication devices, standards for wireless data transmission, topologies of wireless networks, multiple access protocols, and multiple access collisions.

The exhibition is detailed with reference to many contemporary literary sources.

Based on the exposition in the educational part, in *Chapter Two "Methodology and Overview"*, The doctoral student has adopted for his research the inovative wireless technology - the IEEE 802.15.4 / - ZigBee standard. The advantages of the standard are explained in detail - low energy consumption, high speed in creating connections, applicability in different types of topologies with a large number of nodes. Integrated circuits that implement this type of technology are also described and a comparative analysis of their parameters is made.

The doctoral student paid special attention to the problems of security of connections. Different types of hacker attacks for unauthorized access to information in the networks, as well as violation of their functionality are considered.

In *Chapter Three - Objectives and Tasks* an analysis of data transmission in various computer networks has been made. The advantages of digital data transmission over analog data transmission are highlighted. The objectives of the study are stated in detail:

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

From the set goals the doctoral student has formulated the following tasks:

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

2. Overview of the different types of protocols and description of their differences - an overview of the topic.
3. Develop various software simulations using different protocols and analyze data transfer and some characteristics of the computer network such as data stability, bandwidth, etc.
4. Application of new mathematical approaches for analysis and forecasting the stability of computer networks and information system in particular.
5. Testing of computer simulations and realization of a hacker attack by analyzing different ways of entropy and the complexity of the attack.

In the *Discussion* part, in the form of a literature review, the methods and approaches for analysis of computer networks and software systems are debated. With commendable diligence the doctoral student has referred to an impressive number of literary sources in the field of dissertation.

The following is a method of hacking a computer system with Raspberry PI by the method of brute force. The PhD student has described in detail how the password of a WiFi network can be "stolen" with the relevant hardware and software.

In accordance with the set goals, in the dissertation computer simulations of different protocols with the Matlab software package are demonstrated. The prospects of the MIMO-OFDM system (Multiple-Input Multiplexing and Orthogonal Frequency Separation) for reducing the side effects of radio interference in urban environments are highlighted. An example of creating such communication with a 16-element linear phased array antenna is presented. The obtained directivity diagrams have spatial selectivity, which reduces the interference of the signals. MUSIC (Multiple Signal Classification) algorithm is used to determine the spatial spectrum, direction and delay of signals.

Research continues with multiport passive network, QoS (Quality of service) traffic planning, Model 802.11ax wireless connection, cable interface or DOCSIS.

Dignity of the dissertation are the presented results of testing a computer system in real time with the software product Evolink.

In addition to the theory, mathematical models for computer system analysis are considered: Game Theory, Catastrophe Theory, Customer Theory.

Of particular interest are the tables with a comparative analysis of hacker attacks on state structures of the Republic of Bulgaria.

In the concluding part, the author has set out his claims for contributions as follows:

1. Problem areas in the field of information exchange in different computer networks have been identified and a systematic review has been made.
2. Various methods of hacker attacks are presented and methods of their protection. This group of attacks includes any attempt to gain unauthorized access to the system. An analysis of the different types of attacks such as:
 - Denial of Service (DoS) attacks: A type of attack that causes loss of service or inability of the network to function.
 - Web attacks: this is any attack that tries to disrupt / alter a website. Two of the most common such attacks are: SQL injection (SQLi).
 - HTTP Session Hijacking: These attacks are a session hijacking.
 - DNS poisoning: This type of attack compromises the DNS server so that users can be redirected to malicious websites.
3. A method of hacker attack using the brute force method has been developed. Implemented with a hybrid computer of the Arduino type. An analysis of the complexity of the attack was made.

4. Mathematical models for the analysis of the stability of the security of a computer network and ways for annals of this system have been developed. Mathematical approaches such as Markov processes, the theory of games with nature using the Bellman principle and the theory of catastrophes were used.
5. In the Matlab software package many simulations have been made to analyze the data transfer in different computer networks and the influence of noise on this transfer.
6. The traffic on the computer network of the Internet provider is analyzed and the main attacks on the provider are systematized.
7. A conceptual analysis of the types of computer attacks and their ways of conducting on budget enterprises has been made.

In my opinion, the listed contributions are of an applied nature and the author's claims are well-founded.

6. Remarks and recommendations

I have the following remarks and recommendations.

The layout of the dissertation is unusual and makes the narrative difficult to comprehend.

At the beginning of the dissertation there is no literature review. To some extent, the Discussion point has the character of such a review.

In most of the dissertation English sources are used and the translation is unclear and with confused word order. Some specific technical terms are translated with Bulgarian synonyms, which are inaccurate.

Mathematical methods are presented quite indiscriminately. There is no explanation in the analytical expressions for the parameters in them, which makes them a bit "detached" from the general exposition in the dissertation.

I would recommend to Eng. Ilian Ivanov to focus on improving their skills in the field of computer networks.

7. Publications

In the materials for the dissertation, Eng. Ilian Ivanov presented a list of four scientific publications, two of which were co-authored in the prestigious library of Web of Science databases. This is a good attestation for the publishing activity of Eng. Ilian Ivanov.

Conclusion:

The proposed dissertation has qualities that are confirmed by the results obtained. The materials provided to me are sufficient to meet the criteria and requirements of NACID. This gives me grounds to propose to the Scientific Jury to award Eng. Ilian Ivanov the educational-scientific degree "Doctor" in the field of higher education 5.3. Communication and computer technology - Computer systems and networks.

Reviewer:

27. 02. 2022

/ prof. eng. Peter Apostolov, ScD/