TECHNICAL UNIVERSITY OF MOLDOVA

With title of manuscript
UZN: 004.738.5.056.5(043.2)

AMEEN ALI

SECURITY ASSURANCE OF THE COMPUTER NETWORKS BASED ON SOFTWARE DEFINED NETWORK TECHNOLOGIES

Summary of PhD thesis in Engineering Sciences

SPECIALTY 232.01 CONTROL SYSTEMS, COMPUTERS AND INFORMATION NETWORKS

CHISINAU 2025

PhD thesis has been elaborated at the Department of Computer Science and Systems Engineering of the Technical University of Moldova.

Scientific Supervisor:
PERJU Veaceslav, dr. hab., acad. IIA

Members of Guidance Commission:
GUȚULEAC Emilian, dr. hab., univ. prof.
ABABII Victor, dr, assoc. prof.
SUDACEVSCHI Viorica, dr, assoc. prof.

Doctoral commission:
LEAHU Alexei, dr., univ. prof., TUM, President of the PSC of DT.
IZVOREANU Bartolomeu, dr., assoc. prof., TUM, Scientific secretary.
PERJU Veaceslav, dr. hab., acad. IIA, Armed Forces Military Academy, member.
CIORBA Dumitru, dr., assoc. prof., TUM, official reference.
SUDACEVSCHI Viorica, dr., assoc. prof., TUM, official reference.
OHRIMENCO Serghei, dr. hab., univ. prof., AESM, official reference.
ZGUREANU Aureliu, dr., assoc. prof., AESM, official reference.

The sustaining of the thesis will be held on **15.05.2025** at **14:00** during the session of the Doctoral commission at the Technical University of Moldova, Str. Studenților, 9/7, building nr. 3, Faculty of Computers, Informatics and Microelectronics, conf. classroom **3-208**, MD-2045, Chișinău, Republic of Moldova.

PhD thesis and Summary can be consulted in the Scientific Library of the Technical University of Moldova and on the web page of ANACEC.

Summery was sent on **11.04.2025**.

Scientific secretary of the Doctoral commission:
IZVOREANU Bartolomeu, dr., assoc. prof.

Scientific Supervisor:
PERJU Veaceslav, Dr. hab., Acad. IIA

Author:
AMEEN Ali, Eng., M. Sc.

CONTENTS

CONCEPTUAL GUIDELINES OF THE THESIS

The actuality and scientific significance of the research stems from the need to develop better computer networks' infrastructure to deal with the ever-evolving security and data challenges and is supported by analyzing, specifying and defining the theoretical principles of the classical structure of computer networks, SDN structure, cyber-security standards, and the essential concepts of the algorithms like VPN, RSA, and Blockchain.

The importance and relevance of the studied problem consists of elaboration of a new suite of algorithms and SDN controllers' topologies to increase the security level of the SDN topologies and elaboration of the theoretical assessment of computer networks' security level. The SDN comes as a solution to some problems but, with it comes new challenges and from that stems the importance of this study, which is to assure a better security level for SDN structures and which means a better security level for computer networks that use the SDN paradigm.

The main purpose of the thesis is to propose the new solutions to increase the security level of the Software-Defined Network by a suite of new algorithms and SDN controllers' topologies for securing data exchanged between multiple nodes, and to elaborate the methodology of the computer network security level evaluation.

The research objectives:

1. Analysis of existing methods and technologies for security assurance of computer networks.
2. Elaboration of security algorithms to provide the SDN topologies with a better protection against cyber-attacks.
3. Elaboration of SDN controllers' topologies for assuring the security of computer networks.
4. Elaboration of the new method of computer networks' security assessment.
5. Evaluation of security efficiency of the proposed SDN controllers' topologies for computer networks security assuring.

The Hypothesis of the research. As the possible solution for the research problems can be elaboration of the new, more effective algorithms for securing the data exchanged between multiple nodes in SDN networks, of the new kinds of the SDN controllers' topologies for assuring the networks security, and of the theoretical basis of the computer networks security level assessment.

Applied methods of the research consist of the methods of cryptography, modeling and simulation, usage of Petri Nets to research the reliability of the proposed approaches of security assurance, security risk assessment law, general economic cost-related data processing.

The scientific novelty of the obtained results consist of elaborated new algorithms for assuring the security of SDN structures – algorithms Hydra, VPN, Double RSA, and distributed ledger of Blockchain; the elaboration of new controllers' topologies, which are Serial, Parallel and Hybrid topologies; the elaboration of the new method of SDN technology security evaluation based on Petri Nets using and proposed parameters, which are Reliability of Service, Defense Factor, Risk Factor, the Modified Risk assessment and the Cost Effect.

Theoretical significance represents the cryptographic algorithms for assuring the SDN security, such as the Hydra framework, the secured channel of VPN algorithm, Double RSA algorithm, and Distributed ledger of Blockchain algorithm; new topologies of SDN controllers for increasing the security level of computer networks; new method to evaluate the security level of the computer networks, based on using Petri Nets and a set of parameters.

Important scientific solved problem represents the elaboration of a new set of the security algorithms and SDN controllers' topologies to increase the security level of SDN structures and elaboration of the theory of computer networks' security level assessment.

Applicative value of the work is determined by the developed SDN framework based on proposed new algorithms to deal with the centralization issue and by protecting the connection between multiple controllers, which has a big contribution for the SDN community. Also, provides a better view of the security level of a network by measuring it using mathematical tools, based on the proposed parameters.

Scientific results submitted for sustaining.

1. The algorithms to provide the SDN networks with higher level of security: algorithms' suite integrated in Hydra framework, secured channel of VPN algorithm, double RSA algorithm and, distributed ledger of Blockchain algorithm.
2. The SDN controllers' topologies for assuring the security of computer networks Serial, Parallel, and Hybrid kind.
3. The method of the computer networks security level evaluation based on the Petri Nets and a set of proposed parameters: Reliability of Service, Defense Factor, Risk Factor, Modified Risk Factor, and Cost Effect.

Results approval. The results of the research were published in 13 scientific articles, among which 8 by a single author, with a total volume over 7 sheets of author, including 8 in

journals of category B+, 4 - in journal of category B, 1- in journal of category C, and were reported at 5 international and 1 national conferences.

The conferences at which were presented the results: Technical-Scientific Conference of TUM, 2019; International Conference “Security Strategic Environment: Trends and Challenges SSETC-2019”, 2021, Armed Forces Military Academy; International conference on Electronics Communications and computing, 2020, TUM; International Scientific Conference "Evolution of Military Science in the Context of New Threats to National and Regional Security", 2020, Armed Forces Military Academy; International Scientific Conference "The Republic of Moldova in the context of the new regional security architecture", 2024, Armed Forces Military Academy.

Structure and volume of the thesis. The thesis consists of Introduction, **3** chapters, general conclusions and recommendations, bibliography of **130** titles, The main text contains **153** pages, includes **47** figures, **23** tables, **31** formulas and **6** annexes. The volume of the basic compartments is of **105** pages. The results were published in **13** scientific articles.

Keywords: security, assurance, computer network, SDN, algorithm, controller, blockchain, double RSA, Petri Nets

CONTENTS OF THE THESIS

INTRODUCTION

The Introduction reflects the theoretical and practical premises, which emphasize the topicality and importance of the researched problem. The purpose and objectives of the research are formulated, the research hypothesis, the theoretical and practical value of the thesis are described.

1 ANALYSIS OF EXISTING METHODS AND TECHNOLOGIES FOR SECURITY ASSURANCE OF COMPUTER NETWORKS

Chapter 1 provides an overview of the current state of computer networks, covering their structure and hierarchy. It then focuses on software-defined networking (SDN), discussing its structure, history, advantages, and associated security challenges. This chapter highlights SDN's potential for integration with other technologies, showcasing its significance in addressing evolving security threats. Ethane project [1], which introduced the separation of control and data planes, is discussed as the foundation for SDN.

The comparison between the structure of classic networks and software defined networks is made. There are two factors that determine the main differences between traditional network configurations versus SDN one:

1. Network functionality is mainly supported by a dedicated appliance or device. In this

case, dedicated appliance means one or multiple switches, routers and/or application delivery controllers.

2. Most functionality within this apparatus is implemented in dedicated hardware. ASIC (Application specific integrated circuit) will be used for this purpose. Organizations are increasingly confronted with the limitations that accompany this hardware-centric approach, such as traditional configuration is time-consuming and error-prone: Many steps are needed when an IT administrator needs to add or remove a single device in a traditional network [2]. First, here will have to manually configure multiple devices (switches, routers, firewalls) on a device-by-device basis. The next step is using device-level management tools to update numerous configuration settings, such as ACLs, VLANs and Quality of Service. This configuration method makes it harder for administrators to apply consistent policies, leading to potential security breaches and compliance issues.

In short, traditional configurations create significant challenges in meeting business networking standards. Multi-vendor environments require a high level of expertise. The network admin will need to acquire comprehensive knowledge of all device types and vendors in order to successfully configure and set the network. Traditional architectures complicate network segmentation, especially with the growing connectivity of devices like alarm systems and security cameras, in addition to tablets, PCs, and smartphones.

SDN simplifies this by enabling virtual networks, separate from the physical infrastructure. The combination of the network-wide view and the network programmability supports a process of harvesting intelligence from existing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), for example, followed by analysis and centralized reprogramming of the network. This approach can render the SDN more robust to malicious attack than traditional networks [3].

2 ELABORATION OF ALGORITHMS AND TOPOLOGIES FOR ASSURING THE SECURITY OF COMPUTER NETWORKS

Chapter 2 explains the new solutions for the issues in SDN are proposed, which are represented by the key algorithms and techniques forming an integrated framework to enhance SDN security. The main issues noticed in the SDN structure were determined that motivated this research:

1. Centralization: While the centralization of SDN architecture is a key advantage over classical models, it also poses a potential threat by creating a single point of failure (SPOF).

2. East-westbound API: there is not much concentration on them, and it could be

vulnerable to some cyber-attacks like MITM, DDoS or DoS types of attacks [4], [5], [6].

Algorithms for SDN Security assuring based on Cryptography.

1. Algorithms' suite integrated in Hydra framework to counter the Denial of Service / Distributed Denial of Service (DoS/DDoS) attacks [7], by installing botnets [8], [9] on network computers connected to the controller that has the Hydra software installed on it, to make them as potential zombie guards to attack the attacker's source IP. The flowchart diagram of the Hydra framework is shown in the Figure 1.

2. Secured channel of VPN algorithm. A virtual private network (VPN) uses Internet Protocol Security (IPsec), creating secure virtual communication channels. It can be integrated into the proposed framework. A VPN is needed to specify a certainty that the confidentiality of sensitive data can be kept transmitted on the network a Local Area Network (LAN) or workable so that only authorized users are able to access sensitive data [10]. Basically, the research proposes to connect every two controllers using the secure channel of VPN even if they were in the same building. The flowchart diagram of the VPN algorithm is shown in the Figure 2.

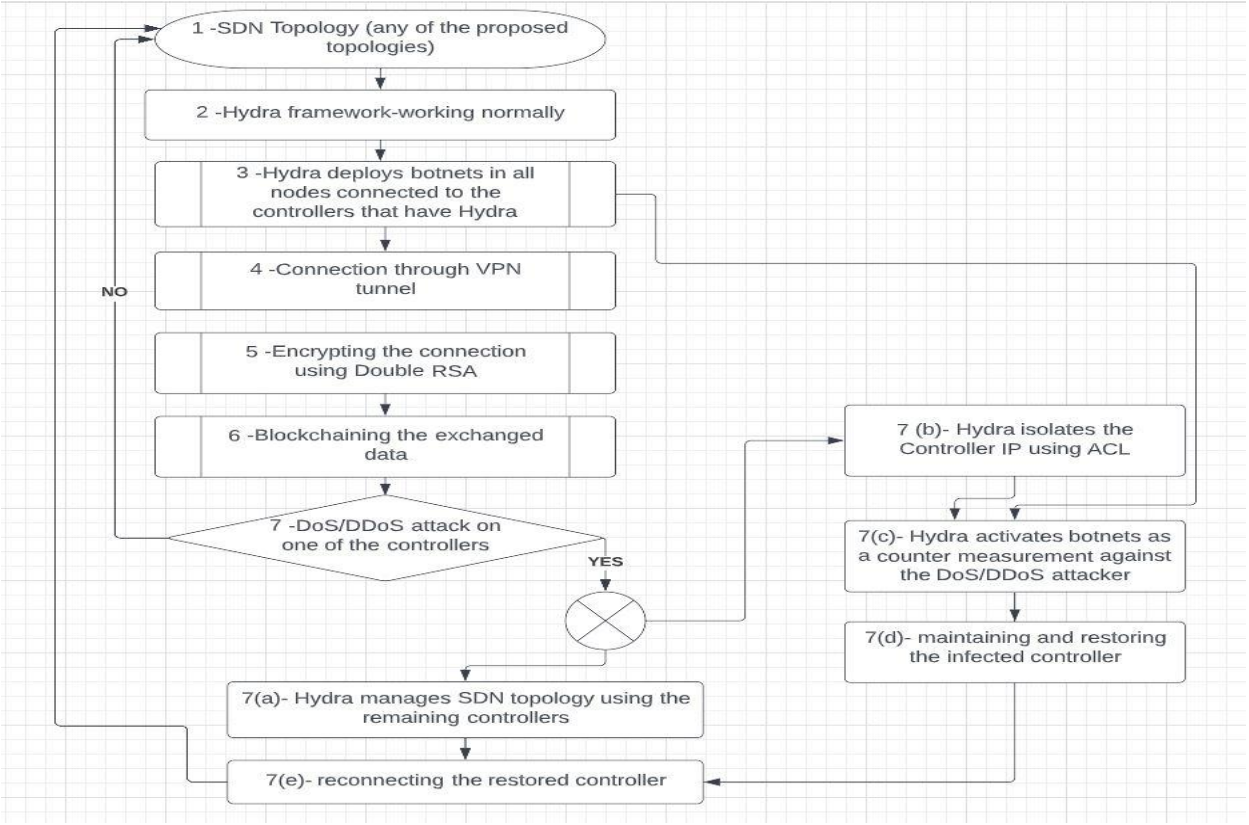

Figure 1. The flowchart diagram of the Hydra framework.

3. Double RSA algorithm. This algorithm represents the RSA by adding another pair of keys for digital signatures in the channel of cryptography; meaning that there will be two pairs of keys, one pair for every encryption-decryption procedure hence; two channels of authentication.

If it is proved to be true that any method to break RSA maybe educe an effective algorithm to factor big integer, it's possible to draw a conclusion that breaking RSA and integer-factor-problem are with the same degree difficulty [11]. The flowchart diagram of the Double RSA algorithm is shown in Figure 3.

4. Distributed ledger of Blockchain algorithm. This algorithm is incorporated in SDN framework to secure the configuration updates between multiple controllers and this is used in a different way from the Marconi protocol [12]. The flowchart diagram of the distributed ledger of Blockchain algorithm is shown in Figure 4.

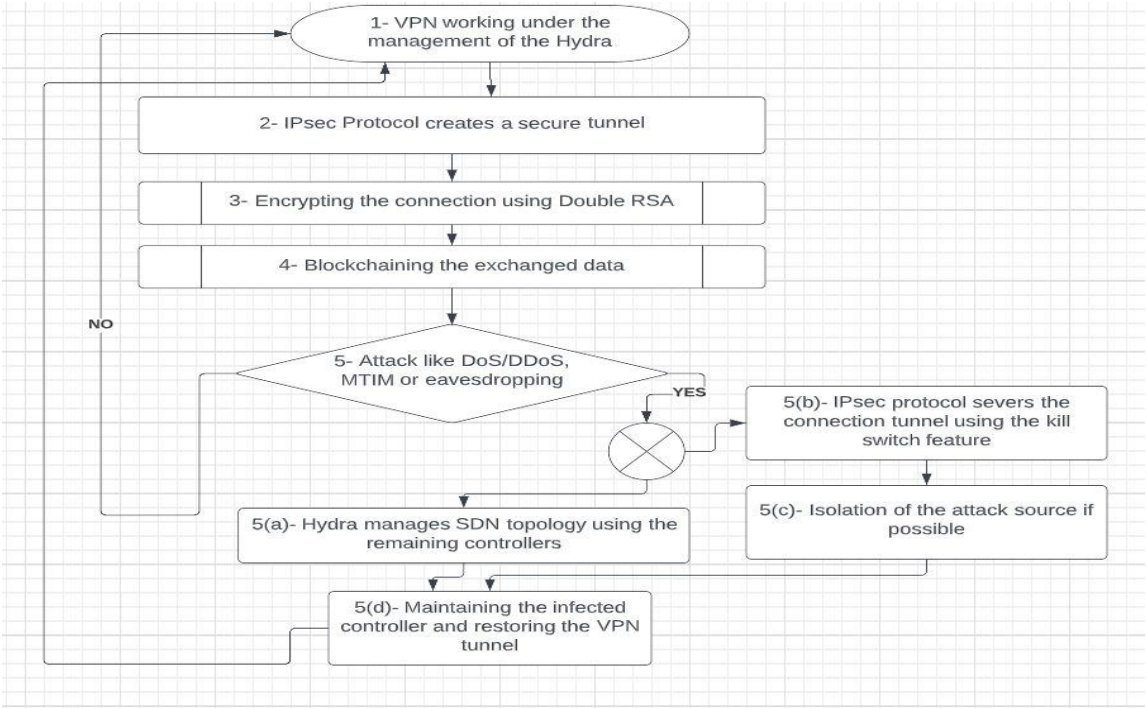

Figure 2. The flowchart diagram of the VPN algorithm.

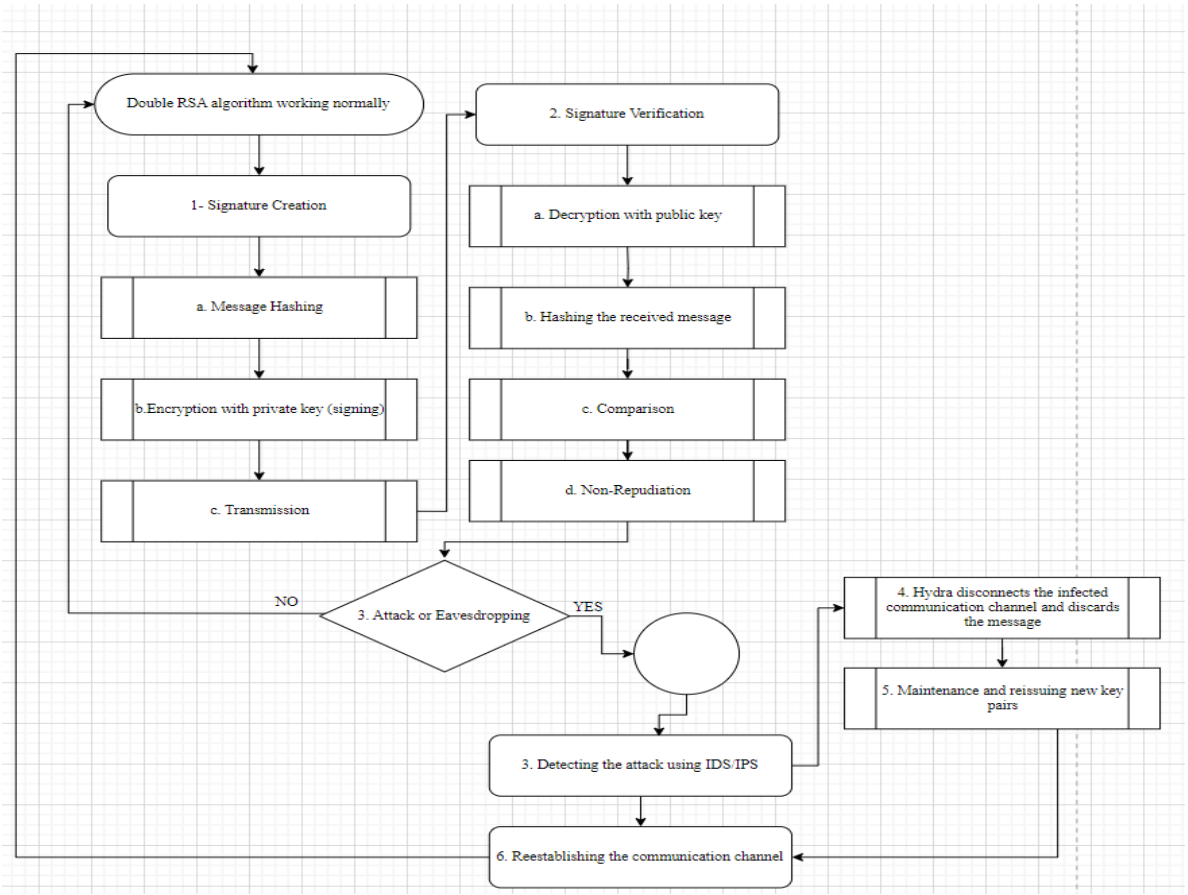

Figure 3. The flowchart diagram of the Double RSA algorithm.

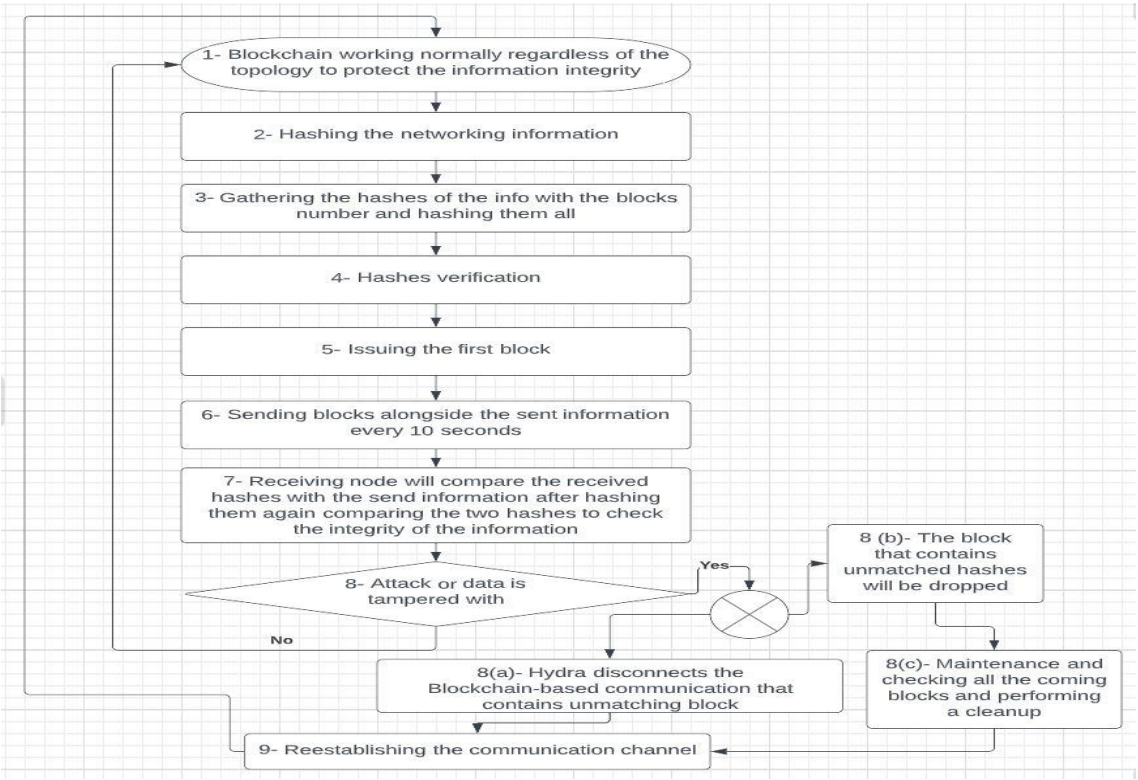

Figure 4. The flowchart diagram of the distributed ledger of Blockchain algorithm.

Topologies proposed for assuring the security of SDN.

In this research various topologies to address the centralization issue are proposed, offering an advantage over traditional network structures. While a software-defined network (SDN) simplifies management and policy enforcement, its single controller can be a single point of failure (SPOF) if attacked. The proposed topologies, which may or may not activate the Hydra framework, help mitigate centralization by varying the number of controllers and their interactions. Although some of these topologies are partially used in other research, the key difference here lies in the interaction between the controllers.

1. **Serial Topology.** The research outlines a serial topology with one main controller and two backups to ensure network continuity during attacks. The main controller updates backups every 10 seconds; delays indicate a potential DDoS attack, prompting a takeover by the backup. As part of the Hydra framework, controllers deploy botnets for countermeasures against attackers. The Serial topology is shown in the Figure 5.**Figure 6. Parallel Topology**

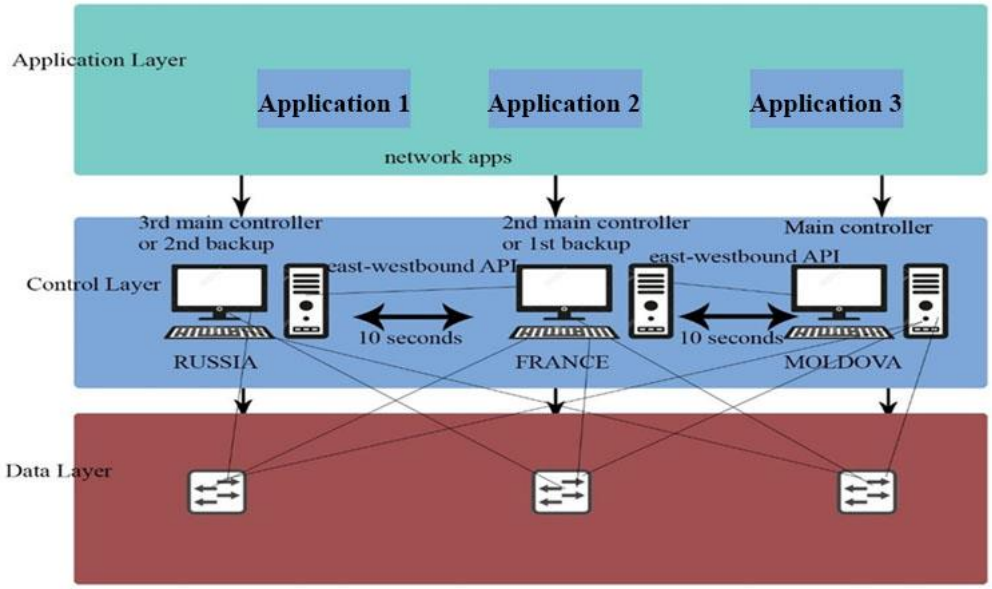

Figure 5. Serial Topology.

2. **Parallel Topology.** In parallel topology, three controllers operate as a unified unit, processing information synchronously and prioritizing nearby network segments without strict hierarchy. They send updates every 10 seconds, and in a DoS/DDoS attack, controllers can isolate the infected one, share its load, or counterattack to maintain network integrity. The parallel topology is shown in the Figure 6.

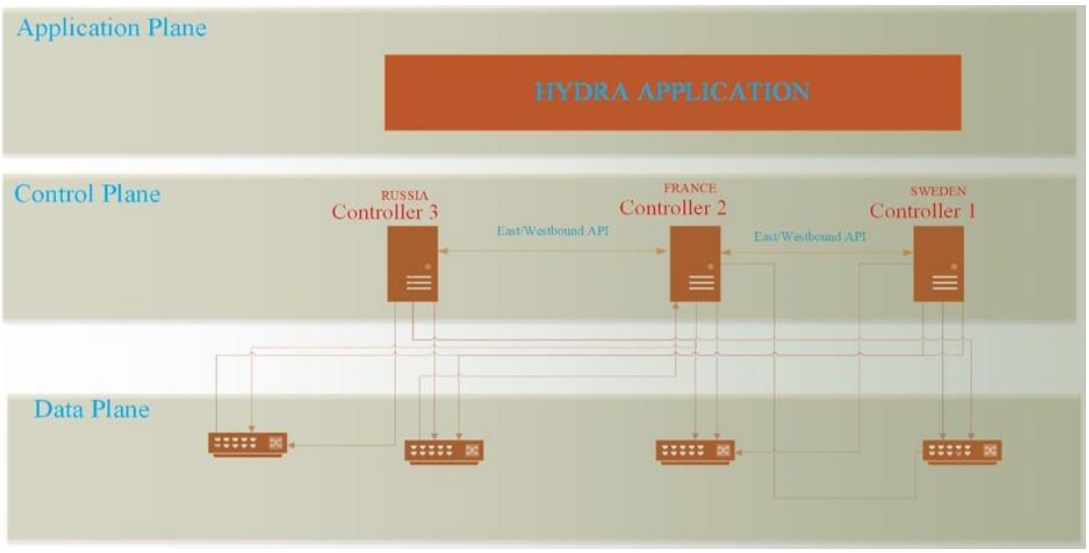

Figure 6. Parallel Topology

3. Hybrid Topology. This topology combines previous designs with six controllers, three primary controllers connected in parallel, each paired with a backup that activates upon failure. Updates are sent every 10 seconds, and backups maintain connections with their primaries and other backups. The Figure 7 shows the Hybrid topology.

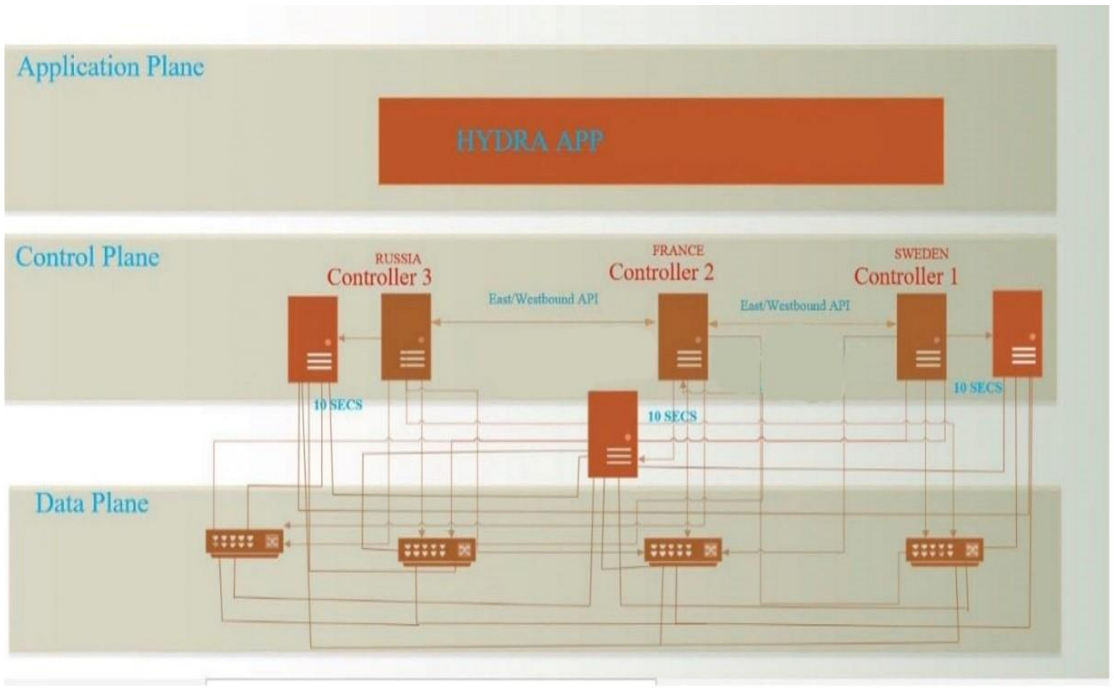

Figure 7. Hybrid Topology.

4. Ordinary Topology. This basic software-defined network topology relies on a single controller to manage switches and computers, risking failure during high demand or a

DoS/DDoS attack. Without a backup, such an attack could compromise the controller, threatening network security and recovery [13], [14]. The Figure 8 shows the Ordinary topology.

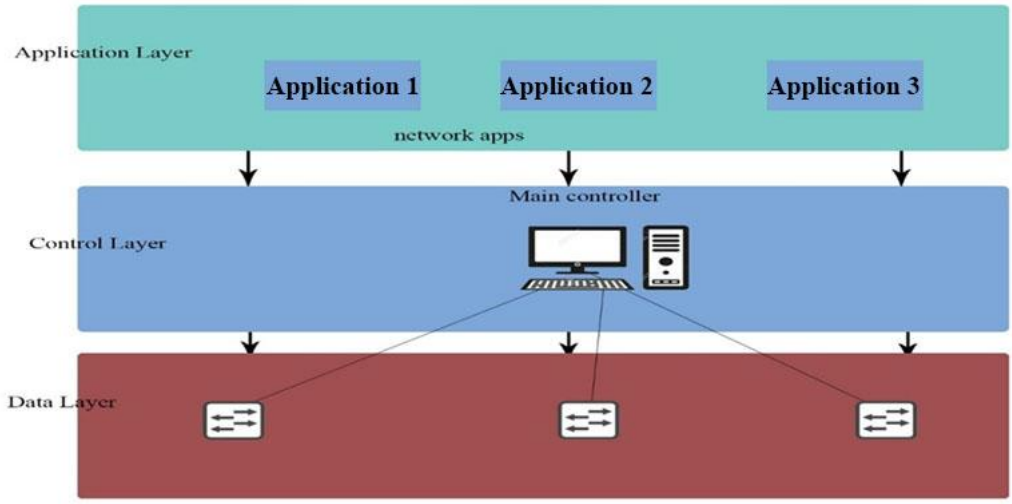

Figure 8. Ordinary Topology.

3 EFFICIENCY EVALUATION OF THE PROPOSED TOPOLOGIES FOR COMPUTER NETWORKS SECURITY ASSURING

Chapter 3 is dedicated to evaluation of the proposed controllers' topologies for network's security protection. The new method of the computer networks security level evaluation based on the usage of the Petri Nets and a set of parameters was elaborated. The Petri Nets modeling of the proposed SDN topologies was made. The simulation of the topologies using Generalized Stochastic Petri Nets module was executed. Determining the efficiency of the topologies using a set of parameters was made.

The method of the computer networks security level evaluation based on the Petri Nets and a set of parameters.

The proposed method consists of the 3 stages. At the **first stage**, for topology of SDN controller to be investigated, a Petri Nets model is elaborated. At the **second stage**, the simulation of the elaborated model is performed using the Generalized Stochastic Petri Nets (GSPN) module which is a 6-tuple (P, T, F, W, M_0, λ), where $P = \{P_1, P_2 \ldots P_m\}$ is a finite set of places, and obtaining the numerical data regarding the places and tokens.

At the **third stage**, based on the obtained data of the simulation will be calculated the proposed set of parameters, such as Reliability of Service, Defense Factor, Risk Factor, Modified Security Risk, and Cost Effect, which will reflect the security level of SDN. The analysis and interpretation of the obtained results will be made.

Let describe the proposed set of parameters, used for computer network security level evaluation.

Reliability of Service (RoS). Reliability of Service (*RoS*) could be close to Quality of Service (QoS) which is the definition of the performance of any system's service, like a computer network or a cloud computing, etc. The SDN has many positive features, which have attracted the attention of researchers to improve the QoS provisioning of today's various network applications [15]. But RoS is a little bit different and has a more detailed specification tailored for the needs of SDN. We propose to measure the RoS as follows:

$$RoS = 1 - TANR / TANR_{O.} \quad (1)$$

Where TANR is the Total Average Number of network requests of the proposed topologies, which is the summation of all averages after dividing them by the count of these averages and that means how many requests per server and shows the risk occurrence level. The $TANR_O$ is the Total Average Number or intensity of requests in controller of ordinary topology.

Defense Factor (DF). Defense Factor (*DF*) can be used to determine the strength and security feasibility of the network against DoS/DDoS attacks. In terms of Petri Nets, the requests will be represented by how many tokens are there in specific places which in turn represent specific nodes in the software-defined network and those specific nodes of interest are the SDN controllers. In the equation (4), the places representing the SDN controllers are denoted as K, where $K \in P$, P is the whole group of places in the Petri Nets (PN) model, which in turn is a tuple of 5 objects, $PN = \{P, T, I, O, M_0\}$[16], where P is the finite set of places, T is a finite set of transitions, I is the input function, O is output function and M_0 is the initial marking.

$$K = \sum_{i=1}^{i=n} Ki,\ K_i \in \{1 - n\}. \quad (2)$$

$$Z = \sum_{i=1}^{i=n} Zi,\quad Z_i \in \{0 - \infty\}. \quad (3)$$

$$DF = [\sum_{i=1}^{i=n} Ki] / [\sum_{i=1}^{i=n} Zi] = \sum_{i=1}^{i=n} [\frac{Ki}{Zi}]. \quad (4)$$

Where K is the number of the places that represent the controllers in a specific model, K_i= = (K_1, K_2…K_n) and Z is the value of tokens in those places K_i, Z_i = (0… ∞). The Defense Factor parameter depends mainly on the assessment of the strength of software-defined network's controllers based on their emptiness and that means their readiness and availability to deter any kind of DoS/DDoS attack. Therefore, it is logical to say that the more controllers we have the better the network's capability it is to deter those attacks. That means the more controllers the better and the higher DF value it is and that explains why the DF equation has the places that represent the controllers in numerator position because the number of controllers is proportional

to the value of the DF. While on the other hand we can see that the more tokens that represent the requests, the weaker the network gets and that means the less DF value we will get.

So, the DF value and the number of tokens or requests are inversely proportional and that's why they should be put in the denominator position. In addition, it is mentioning worthy that if we reversed the DF then, meaning if the tokens/requests are divided by the places/controllers then we'll get how many requests per server [17].

Risk Factor (RF). Risk Factor (*RF*) parameter can be used to figure out the weakness level of the network environment. The values of the Total Average Number (distribution intensity) of Requests (*TANR*) can be described as the Risk Factor. Since we need to find the strength and defense ability of the network controllers to deter the DoS/DDoS attacks and the more tokens/ requests we have, the more occupied the controllers will be and the weaker they will be and this way we will not get defense ability or reliability level of the network but rather the weakness point.

So, we propose also the Risk Factor (*RF*) parameter to evaluate the efficiency of the elaborated topologies. The Parameter can be estimated as:

$$RF = 1/DF. \tag{5}$$

where DF is the Defense Factor value of the measured topology. The parameter RF will still be the opposite of what we need to figure out, which is the (*TANR*) also. The places/controllers should be in the numerator and the tokens/requests should be in the denominator and that is another logical proof of why there was a need to derive that formula and to put it in that form.

Modified Security Risk Assessment parameter (RM). To assess the security level of computer networks, it's possible to leverage the risk assessment law but to make it suitable for SDN. Then it's possible to modify the risk assessment law and after modification, it's called in this research, the modified risk assessment (*RM*). Based on the modified law of security risk assessment, we can apply the security risk assessment law [18] to evaluate the protection level of the computer networks, which states:

$$R = P_0 * V. \tag{6}$$

where R is the security risk assessment that quantifies and shows the possibility of a threat acting upon a vulnerability successfully and the severity of the results of that attack, P_0 represents the initial probability or likelihood of the vulnerability occurrence and V represents the value or cost of the asset.

In other words, using this formula we can estimate how much our proposed framework will reduce the security risk of a computer network, hence assuring its security. Since a server is the most important part and has the highest value node in the network environment, in which we

will install our controller software, then we can say it has the highest asset value or impact. The servers have the value V=100 as an asset impact because it is the value of the server's impact on the secure socket layer (SSL) which is the same layer in which the OpenFlow protocol works.

The probability of vulnerability P_0 = 0.025 which is measured based on the lost orders due to the web server denial of service attack. We can gain a new value of probability P_n, which will be affected by the DF mathematically as shown:

$$P_n=P_0/DF. \quad (7)$$

The higher Defense Factor, the better which is the opposite of the probability of vulnerability. That means that they should be inversely proportional mathematically as they're logically and that's why they're positioned this way in the formula of finding the new likelihood or probability of vulnerability.

It is possible to estimate that our framework and the formula derived from its modeling will reduce the likelihood of attacks occurrence (like DoS/DDoS attacks) and for that we propose a modified version of Security Risk Assessment parameter and it will be as:

$$RM = P_n*V. \quad (8)$$

The usage circumstances of these parameters differ from each other. When it is needed to measure the data protection performance then, it is possible to apply the *RoS* parameter. When there's a need to determine the defense ability and the network's strength against DoS/DDoS attacks then, it is possible to depend on the *DF* parameter. While if there was a need to reverse the situation and figure out the weakness of the network then, it is possible to reverse the parameter and use the *RF* which is the inversely proportional to *DF*. In case there was a need to measure the SDN environment weakness based on the computer networks law, then it is possible to modify it to be used based on the proposed SDN environments and their Petri Nets modeling and in this case the *RM* parameter can be used.

Cost Effect parameter (Y). To evaluate the influence of the costs of using the proposed controller topologies for SDN security assurance, we used the data regarding the prices of the switches, computers and controllers [19], [20]. Previously there were described the basic structures of the controllers' topologies - Serial, Parallel, Hybrid and Ordinary. Let estimate the cost of these topologies, taking into account as basic the Ordinary topology, which will include 1 controller, 3 switches and 6 computers. Both the Serial and Parallel topologies will have 3 controllers, 3 switches and 6 computers and the Hybrid topology will contain 6 controllers, 3 switches and 6 computers. In this case, the total cost TC of the Ordinary network topology can be estimated as:

$$TC_O = CC+3SC+6NC. \quad (9)$$

Where, *CC*, *SC* and *NC* are the cost of controller, switch and network computer respectively. The total cost of the Serial and Parallel topologies will be as follows:

$$TCS, P = 3CC+3SC +6NC. \quad (10)$$

And the total cost of the Hybrid topology will be:

$$TC_H = 6CC+3SC+6NC. \quad (11)$$

Let's establish the relations between the costs of the controller, switch, and computer as follows:

$$CC= aSC = bNC. \quad (12)$$

Where parameters $a = \{a_{min} \div a_{max}\}$, *and* $b = \{b_{min} \div b_{max}\}$. If we apply those values in the equations (9 -11) then, the costs of the topologies could be described as:

$$TC_O = CC+3SC+6NC = CC\ (1+3/a+6/b). \quad (13)$$

$$TC_{S,P} = 3CC+3SC +6NC = 3CC\ (1+1/a+2/b). \quad (14)$$

$$TC_H = 6CC+3SC+6NC = CC\ (6+3/a+6/b). \quad (15)$$

The effectiveness of cost difference in using the proposed topologies can be shown by the following formulas:

$$Y1 = TC_{S,P}/TC_O = 3(2a+b+ab)/(6a+3b+ab). \quad (16)$$

$$Y2 = TC_H/TC_O = 3(2a+b+2ab)/(6a+3b+ab). \quad (17)$$

$$Y3 = TC_H/TC_{S,P} = (2a+b+2ab)/(2a+b+ab). \quad (18)$$

Simulation of the proposed controllers' topologies using Generalized Stochastic Petri Nets module.

Using the Generalized Stochastic Petri Nets module in the PIPE software, it was obtained the results regarding the average tokens' number (distribution intensity or how many tokens exist in each place per unit of time) in the places that represent the SDN controllers. The results are presented in the Figure 9.

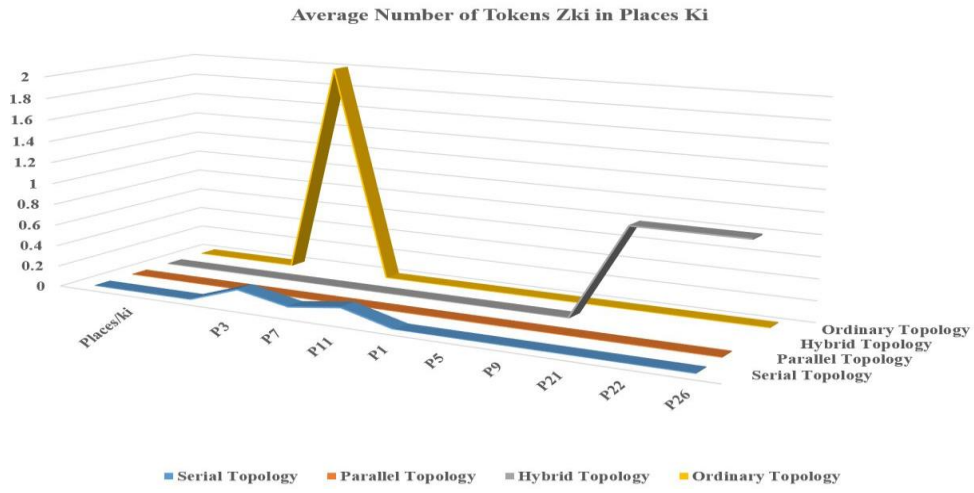

Figure 9. Average number of tokens in places representing the SDN controllers.

From the information taken from the Figure 9, it is possible to infer that the least number of tokens/requests per unit of time lies within the controllers of the Parallel topology, which means that they will be free and available for dealing with requests most of the time and that would mean that they will be more capable of deterring the DoS/DDoS attacks hence. It is possible to say that the best topology of all the proposed topologies would be the Parallel topology while the worst would be the already existing Ordinary Topology due to its high number of tokens and to its dependence on a single controller that could be a point of failure.

Determining the efficiency of the proposed topologies using a set of parameters.

The efficiency of the proposed controllers' topologies will be determined using the parameters Reliability of Service (*RoS*), Defense Factor (*DF*), Risk Factor (*RF*), Modified Risk Assessment (*RM*) and cost effectiveness. The Figure 10 show the values of the parameters of the topologies.

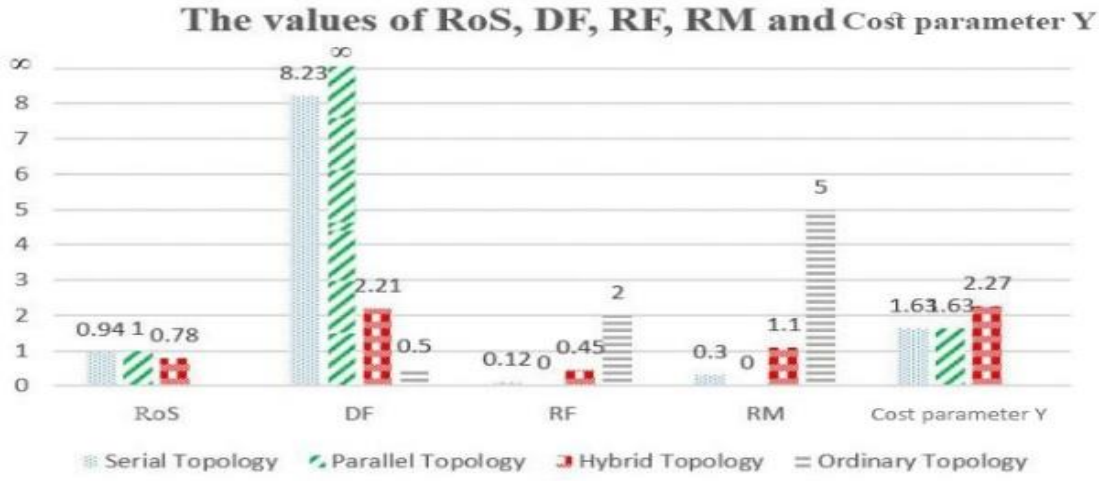

Figure 10. The values of the proposed topologies parameters

From the data presented in Figure 10, it is possible to infer that the Parallel topology is the best one from the point of view of all security estimation parameters, after that comes the Serial topology and the Hybrid topology is the last one.

The usage circumstances of these parameters differ from each other. When it is needed to measure the data protection performance then, it is possible to apply the *RoS* parameter, where the reliability of service of the serial topology is 0.94 of the previous Reliability of service of the single-controller ordinary topology. The parallel topology gained a 100% enhancement as compared to the ordinary topology and the hybrid topology proved to be better than the ordinary topology as well in terms of reliability of service by 0.78. In other words, it is possible to say that the best topology of all the proposed topologies in terms of *RoS*, is the parallel topology.

When there's a need to determine the defense ability and the network's strength against DoS/DDoS attacks then, it is possible to depend on the *DF* parameter. Where the defense factor that shows the strength of presented SDN topologies against DoS/DDoS attacks has the value of 8.23, while the parallel topology has a very high value close to ∞ since the number of the tokens that represent network requests in its controllers, are very small and close to 0 most of the processing time and that means that the defense factor value of this topology is close to optimal, meaning the parallel topology is nearly most reliable against DoS/DDoS attacks, the hybrid topology has a value of 2.21 and last but not least the ordinary topology has the least value which is 0.50, meaning that the single-controller topology has the weakest structure against DoS/DDoS attacks.

While if there was a need to reverse the situation and figure out the weakness of the network then, it is possible to reverse the parameter and use the *RF* which is the inversely proportional to *DF*. So that means the higher the value, the worse it is. It is possible to conclude that the serial topology has the value of 0.12, the risk factor value of the parallel topology is 0 since it is nearly optimal and that means this structure has low risk, the hybrid topology has a risk factor of 0.45 and least but not last the ordinary topology has the highest value of 2.0, which refers to the high jeopardy that comes along the usage of this topology.

In case there was a need to measure the SDN environment weakness based on the computer networks law, then it is possible to modify it to be used based on the proposed SDN environments and their Petri Nets modeling and in this case the *RM* parameter can be used. This parameter is a proof of how the *DF* equation has assured the security of the proposed topologies and reduced the risk value as compared to the already existing ordinary topology in terms of the risk assessment law that is used to describe the security risk for computer networks in general.

So, after modifying the risk assessment law by incorporating the effect of the Defense Factor in its equation to create a new parameter called the Modified Risk parameter, the research shows that the serial topology has a reduced *RM* value of 0.3, the parallel topology has a value of 0 as well hence, it is the best topology of all the suggested topologies, the hybrid topology's *RM* value is 1.1 and the single-controller topology has a value of 5.0 and this high *RM* value of the ordinary topology shows the security enhancements, the proposed topologies have in their design over the ordinary topology.

When there's a need to see the cost effect of using the proposed topologies to assure the security of SDN paradigm as compared to the already-existing single-controller Ordinary topology; then it is possible to check the cost parameter which shows that based on this research and on the specific prices' data gathered; that using of Serial and Parallel topologies prices could

be increasing by maximum 1.63 times as compared to the usage of the Ordinary topology. While using the Hybrid topology could increase the expenses by 2.27 times more than the expenses for the Ordinary topology. To show a more detailed efficiency of the proposed SDN controllers' topologies, it was calculated the relations of the security assessment parameters of the new topologies as compared to the Ordinary topology as follows. Relation of DF of Proposed topologies to the Ordinary topology $R_{DF} = DF_{pr}/DF_{O}$, Relation of RF of the Ordinary topology to the Proposed topologies $R_{RF} = RF_{O}/RF_{pr}$, Relation of RM of the Ordinary topology to the Proposed topologies $R_{RM} = RM_{O}/RM_{pr}$. The results of the calculations are presented in Table 1.

Table 1. The values of parameters for the proposed topologies in comparison with the Ordinary topology

No.	***Topology***	***RoS***	R_{DF}	R_{RF}	R_{RM}	***Y***
1	Serial Topology	0.94	16.46	16.66	16.66	1.63
2	Parallel Topology	1.0	∞	∞	∞	1.63
3	Hybrid Topology	0.78	4.42	4.44	4.54	2.27

From the Table 1 it is possible to infer that Serial topology has a better *RoS* by 0.94, better R_{DF} by16.46 times, less R_{RF} and R_{RM} by 16.66 times and more cost *Y* by 1.63 as compared to the Ordinary topology. On the other hand, the Parallel topology has a better RoS by 100%, better R_{DF} by ∞ times, less R_{RF} and R_{RM} by ∞ times and more cost *Y* by 1.63 as compared to the Ordinary topology. While the Hybrid topology has a better RoS by 0.78, better R_{DF} by 4.42 times, less R_{RF} by 4.44 times, less R_{RM} by 4.54 times and more cost *Y* by 2.27 as compared to the Ordinary topology. The data presented in Table 1 show, that the Parallel topology can be characterized as the topology with the highest value of security protection in comparison with the other topologies. Regarding the cost of the proposed topologies, it was concluded that the Serial and Parallel topologies require the increasing of the cost by 1.63 times as compared to the Ordinary topology and the Hybrid topology by 2.27 times as compared to the Ordinary topology.

The gained mathematical results are mostly theoretical and it is well considered that division over zero is not permissible but due to the results gained by the PIPE software simulation; it was imperative to conduct such a mathematical operation, but this shows that the Parallel topology is very reliable and near optimal.

GENERAL CONCLUSIONS AND RECOMMENDATIONS

GENERAL CONCLUSIONS.

The main scientific results obtained in the research are the following:

1. In the thesis, it was argued the Software-Defined Networking as a potential solution for addressing cyber threats. It was presented a security efficiency evaluation of some of the most prominent SDN-related techniques, researches and methods, which shows the importance of SDN in the technology and its ability to be incorporated with other technologies to enhance them and the flexibility of SDN to accept other technologies in its paradigm to gain more enhancements [21].

This analysis permitted to formulate the problems noticed in the SDN environmental structure, such as Centralization - despite that SDN controllers give the ability to manage the network environment from a single point but that also could be considered as a weakness point if jeopardized and used as a single point of failure.

2. The new cryptographic algorithms were proposed, integrated within technologies for assuring SDN security. The algorithms suite consists of the Hydra framework mainly and integrated within it, the secured channel of VPN algorithm, Double RSA algorithm, and Distributed ledger of Blockchain algorithm. These algorithms work together and interact to form the Hydra-like behavior of the framework to deter Man In The Middle (MITM) attacks and Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks [22].

3. Three topologies of SDN controllers were proposed, which are serial, parallel and hybrid ones, for increasing the security level of networks by adding more controllers that interact in a specific way, to address the issue of Single Point Of Failure (SPOF) [23], [24], [25].

4. The new method proposed for evaluation of the computer networks security level, based on using of the Petri Nets and a set of parameters such as Reliability of Service (*RoS*), Defense Factor (*DF*), Risk Factor (*RF*), Modified Risk assessment parameter (*RM),* and Cost Effect (*Y*) [26].

5. It was established, that when it is needed to measure the data protection performance then, it is possible to apply the *RoS* parameter. When there's a need to determine the defense ability and the network's strength against DoS/DDoS attacks then, it is possible to depend on the *DF* parameter. While if there was a need to determine the weakness of the network then, it is possible to use the parameter *RF*. In case there was a need to measure the SDN environment weakness based on the computer networks law, in this case the *RM* parameter can be used [27].

6. The modeling and simulation of the proposed Serial, Parallel, and Hybrid SDN topologies using Petri Nets and Generalized Stochastic Petri Nets (GSPN), was made. It was shown that it is possible to infer that the least number of tokens/requests lies within the controllers of the Parallel topology per unit of time, which means that they will be free and available for dealing with requests most of the time and that would mean that they will be more capable of deterring the DoS/DDoS attacks hence, it is possible to say that the best topology of all the proposed topologies would be the Parallel topology [28], [29].

7. It was determined, that the Serial and Parallel topologies would have more cost in establishing as compared to the Ordinary topology by 1.63 times and the Hybrid topology's cost increases by 2.27 times as compared to the Ordinary topology [30].

The novelty of the research consists of elaborated new algorithms for assuring the security of SDN, which are Hydra, Double RSA, and distributed ledger of Blockchain; the elaboration of new controllers' topologies, which are Serial, Parallel and Hybrid topologies; the elaboration of a new method of security evaluation of computer networks based on Petri Nets and five parameters which are Reliability of Service, Defense Factor, Risk Factor, the Modified Risk assessment law and the Cost effect of the proposed SDN controllers' topologies.

Applicative value of the work is determined by the developed framework, which has a big contribution for the SDN community by proposing new SDN topologies to deal with the centralization issue and by protecting the connection between multiple SDN controllers. Also, provides a better view for the security level of a specific network by measuring it using various mathematical tools that are based on different proposed parameters.

RECOMMENDATIONS

The research could be stretched and investigated deeper in various directions, like:

1. The possibility to enhance the usage circumstance for the proposed parameters and make them more often used and more capable to measure the security level of the data plane of the software-defined network structure.
2. Securing TLS/SSL against DoS, as know the controller communicates with the switches through the transport layer using protocols like openflow.
3. Using neural networks and artificial intelligence to create an analytical algorithm for detecting anomalies based on the statistics, and that algorithm could be built on top of a framework that is integrated with the controller.
4. Usage of data mining to calculate mistake, problems, attacks, network issues, code

errors and human mistake; all those statistics combined with the previous article of AI to create a self-sufficient and self-protecting computer network that uses the SDN structure.

5. Adding more controllers in the proposed topologies could considered as enhancement, especially if there were more new simulations using different approaches to gain new better results.

REFERENCES

1. CASADO, M, et. al. Ethane: taking control of the enterprise, In: *ACM SIGCOMM Computer Communication Review*, 2007, 37(4), pp. 1–12.
2. IP knowledge. (2013). traditional VS SDN [whitepaper].
3. SCOTT-HAYWARD, S, O'CALLAGHAN, G, SEZER, S. SDN Security: A Survey. In: *IEEE SDN for Future Networks and Services (SDN4FNS)*, 2013, Centre for Secure Information Technology (CSIT), (10), pp. 1-7.
4. AYESHA, I. SDN controllers' security issues: MS thesis. *University of Jyväskylä* - Finland, 2017.
5. MALIK, A, AHSAN, A, SHAHADAT, M, TSOU, J. Man-in-the-middle-attack: Understanding in simple words. In: *International Journal of Data and Network Science*, 2019, 3, pp. 77-92.
6. PRASAD, K, REDDY, A, RAO, K. DoS and DDoS Attacks: Defense, Detection and Trace Back Mechanisms – A Survey. In: *Global journal of computer science and technology: E Network, Web and Security*, 2014, 14 (7), pp. 15-32.
7. BAWANY, N, SHAMSI, J, SALAH, K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. In: *Journal of Cryptology*, 2017, 42, pp. 425-441.
8. OSAGIE, M, ENAGBONMA, O, INYANG, A. the historical perspective of botnet tools. In: *Current Journal of Applied Science and Technology*, 2019, 32 (6), pp. 1-8.
9. CCTV-based botnet used for DDoS attacks. [Online]. [Accessed: 04.07.2017]. Available: https://www.ddosattacks.net/a-massive-botnet-of-cctv-cameras-involved-inferocious-ddos-attacks .
10. IQBAL, M, RIADI, I. Analysis of Security Virtual Private Network (VPN) Using OpenVPN. In: *International Journal of Cyber-Security and Digital Forensics*, 2019, 8 (1), pp. 58-65.
11. TAN, W, et. al. Analysis of RSA based on Quantitating key security strength. In: *Procedia Engineering*, 2011, 15, pp. 1340-1344.
12. How blockchain will manage networks. [Online]. 2019, [accessed: 26.08.2019] available: https://www.networkworld.com/article/3356496/how-blockchain-will-manage-networks.html.
13. **AMEEN, A.** Software - Defined Networks. A General Survey and Analysis, In: *Journal of Engineering Science*, 2018, 25 (3), pp. 61-73.

14. **AMEEN, A.** The Using of SDN Technologies for Security Insurance of Computer Networks, In: proc. of *Technical-Scientific Conference of TUM*, 2019, Technical University of Moldova, 1, pp.1-4.
15. KARAKUS, M, DURRESI, A. Quality of Service (QoS) in Software Defined Networking SDN: A Survey. In: *Journal of Network and Computer Applications*, 2017, 80, pp. 200-218.
16. ALMUTAIRI, L, SHETTY, S. Generalized Stochastic Petri Net Model Based Security Risk Assessment of Software Defined Networks. In: *IEEE Military Communications Conference*, 2017, pp. 545-550.
17. PERJU, V, **AMEEN, A.** State Security Assurance through the Creation of High-Protected Computer Networks, In proc. of *International Conference "Security Strategic Environment: Trends and Challenges SSETC-2019"*, 2021, Armed Forces Military Academy, pp. 101-109.
18. WHITMAN, M, MATTORD, H. Principles of Information Security (book). USA, 2011. 658 p. ISBN-13: 978-1-111-13821-9.
19. Dell Poweredge Servers Special Deals and Offers. [Online]. 2022, [Cited: 02.06.2022] available: https://www.dell.com/en-uk/work/shop/deals/enterprise-deals.
20. Cisco Switch Catalyst 1000. [Online]. 2022, [Cited: 02.06.2022] available: https://www.router-switch.com/cisco-catalyst-1000-switches-price.html.
21. **AMEEN, A.** Leveraging Blockchain Technology to Assure Security of SDN, In: proc. of *International conference on Electronics Communications and computing*, 2020, pp. 1-12.
22. **AMEEN, A.** Making Cyber Space Networks a Safer Work Environment After Covid-19 Using Software-Defined Networks' Technologies, In: proc. of *International scientific conference-evolution of military science in the context of new threats to national and regional security*, 2020, Armed Forces Military Academy, volume 1, pp. 246-260.
23. **AMEEN, A.** Assuring the SDN security by modeling and comparing SDN proposed topologies using Petri Nets. In: *Journal of Engineering Science*, 2021, 28(4), pp. 93-105.
24. **AMEEN, A.** MODELING PROPOSED SDN PARALLEL TOPOLOGY AND EVALUATION OF ITS RELIABILITY. In: *Polish Journal of Science*, 2023, (66), pp. 47-56.
25. **AMEEN, A.** modeling proposed hybrid software-defined network controllers' topology by using Petri Nets system. In: *Studia Universitatis Moldaviae*, 2021, 2(142), pp. 40-50.

26. PERJU, V, Mastac, I, **AMEEN, A.** Modern Military Command and Control Systems and their Security Ensuring based on the SDN technology. In: *Polish Journal of Science*, 2023, (69), pp. 45-51.
27. PERJU, V, **AMEEN, A.** Security Assurance of State-of-the-Art Military Command-and-Control Systems Using the SDN-Based Technologies. In: Proc. of *International Scientific Conference "Republic of Moldova in the context of the new regional security architecture"*, 2022, Armed Forces Military Academy, 1, pp. 169-182.
28. **AMEEN, A**, Guţuleac, E. Petri Nets Modeling for SDN topologies. In: *Journal of Engineering Science*, 2021, 28(2), pp.79-90.
29. **AMEEN, A.** Evaluation of the Computer Networks Security Level Based on Petri Nets & a Set of Parameters. In: *Polish Journal of Science*, 2023, (68), pp. 82-91.
30. PERJU, V, **AMEEN, A.** ASSESSING THE SECURITY OF MILITARY COMPUTER NETWORKS BASED ON THE PETRI NETS MODELING AND A SET OF PARAMETERS. In: Proc. of *International Scientific Conference "The Republic of Moldova in the context of the new regional security architecture"*, 2024, Armed Forces Military Academy (to be published).

LIST OF PUBLISHED WORKS

1. AMEEN, A. Software - Defined Networks. A General Survey and Analysis, In: *Journal of Engineering Science*, 2018, 25 (3), pp. 61-73. DOI: https://doi.org/10.5281/zenodo.2557306.
2. AMEEN, A. The Using of SDN Technologies for Security Insurance of Computer Networks, In: proc. of *Technical-Scientific Conference of TUM*, 2019, Technical University of Moldova, 1, pp.1-4. https://ibn.idsi.md/en/vizualizare_articol/84710n.
3. PERJU, V, AMEEN, A. State Security Assurance through the Creation of High-Protected Computer Networks, In proc. Of *the International Conference "Security Strategic Environment: Trends and Challenges SSETC-2019"*, 2021, Armed Forces Military Academy, pp. 101-109.
4. AMEEN, A. Leveraging Blockchain Technology to Assure Security of SDN, In: proc. of *International conference on Electronics Communications and computing*, 2020, Technical University of Moldova, pp. 1-12. DOI: https://doi.org/10.5281/zenodo.4288305.
5. AMEEN, A, GUŢULEAC, E. Petri Nets Modeling for SDN topologies. In: *Journal of Engineering Science*, 2021, 28(2), pp.79-90.
   DOI: https://doi.org/10.52326/jes.utm.2021.28(2).06.
6. AMEEN, A. modeling proposed hybrid software-defined network controllers' topology by using Petri Nets system. In: *Studia Universitatis Moldaviae*, 2021, 2(142), pp. 40-50. DOI: https://doi.org/10.5281/zenodo.5094689.
7. AMEEN, A. Making Cyber Space Networks a Safer Work Environment After Covid-19 Using Software-Defined Networks' Technologies, In: proc. of *International Scientific Conference-Evolution of Military Science in the Context of New Threats to National and Regional Security*, 2020, Armed Forces Military Academy, volume 1, pp. 246-260.
   https://ibn.idsi.md/vizualizare_articol/162231.
8. AMEEN, A. MODELING PROPOSED SDN PARALLEL TOPOLOGY AND EVALUATION OF ITS RELIABILITY. In: *Polish Journal of Science*, 2023, (66), pp. 47-56. https://doi.org/10.5281/zenodo.8337094.
9. AMEEN, A. Assuring the SDN security by modeling and comparing SDN proposed topologies using Petri Nets. In: *Journal of Engineering Science*, 2021, 28(4), pp. 93-105. https://doi.org/10.52326/jes.utm.2021.28(4).08.
10. PERJU, V, Mastac, Ion, AMEEN, A. Modern Military Command and Control Systems and their Security Ensuring based on the SDN Technology. In: *Polish Journal of Science*, 2023, (69), pp. 45-51. DOI: https://doi.org/10.5281/zenodo.10400324.
11. AMEEN, A. Evaluation of the Computer Networks Security Level Based on Petri Nets & a Set of Parameters. In: *Polish Journal of Science*, 2023, (68), pp. 82-91.

DOI: https://doi.org/10.5281/zenodo.10132797.

12. PERJU, V, AMEEN, A. Security Assurance of State-of-the-Art Military Command-and-Control Systems Using the SDN-Based Technologies. In: Proc. of *International Scientific Conference "Republic of Moldova in the context of the new regional security architecture"*, 2023, Armed Forces Military Academy, 1, pp. 169-182.
13. PERJU, V, AMEEN, A. ASSESSING THE SECURITY OF MILITARY COMPUTER NETWORKS BASED ON THE PETRI NETS MODELING AND A SET OF PARAMETERS. In: Proc. of *International Scientific Conference "The Republic of Moldova in the context of the new regional security architecture"*, 2024, Armed Forces Military Academy, (to be published).

ANNOTATION

To the doctoral dissertation "**Security assurance of the computer networks based on software defined network technologies**" is submitted by Mr. Ali AMEEN for fulfillment of the requirements for the PhD in Engineering Sciences, specialty 232.01– *Control system, computers and information networks.* The dissertation was prepared at the Technical University of Moldova.

The structure of the thesis. The thesis contains Introduction, **3** chapters, general conclusions and recommendations, bibliography of **130** titles. The main text contains **117** pages, includes **47** figures, **23** tables, and **6** annexes. The obtained results of the thesis were published in **13** scientific papers.

Keywords: Software-Defined Networks (SDN), OpenFlow, security, controller, Hydra, virtual private network (VPN), Rivest-Shamir-Adleman (RSA), Blockchain.

Research problem: assuring the security of SDN-based computer networks.

Aim of research is to outline the current security state of the computer networks and to suggest new solutions to patch up different security aspects.

The objectives of thesis include analysis of existing methods and technologies for security assurance of computer networks, elaboration of algorithms and topologies for incresing the security assuring level of computer networks and efficiency evaluation of the proposed topologies for computer network security assuring.

Scientific novelty and originality of the obtained results are reflected in a new framework that assures the security of SDN and uses different techniques combined together to deal with the single point of failure in the SDN architecture, adds a defense mechanism by injecting the attacking source with botnets. And the usage of Petri Nets modeling technique to figure out the best outcome of the proposed topologies and to get different performance parameters that are translated to equations based on that modeling of those specific topologies to determine the one with the best performance in terms of cost saving and deterrence to cyber-threats like DoS/DDoS attacks.

Important scientific solved problem consists in elaboration of a new suite of algorithms and SDN controllers' topologies to increase the security level of SDN and elaboration of the theoretical assessment of computer networks' security level.

Theoretical significance can be described by defining the main problems in security assurance of the computer networks, by specifying the main issues in the SDN paradigm that need to be patched, the theoritization of the essential concepts of the proposed algorithms and topologies.

Applicative value of the work is determined by the developed framework, which has a big contribution for the SDN community by proposing new SDN topologies to deal with the centralization issue and by protecting the connection between multiple SDN controllers. Also, provides a better view for the security level of a specific network by measuring it using various mathematical tools that are based on proposed parameters.

Implementation of results. The obtained results were used in Dekart Company's investigations regarding the new approaches in information security.

ADNOTARE

La teza de doctor **„Asigurarea securitatii retelelor de calculatoare bazate pe tehnologii de rețea definite software”** este prezentată de domnul Ali AMEEN pentru conferirea titlului științific de doctor în Științe Inginerești la specialitatea 232.01– Sisteme de conducere, calculatoare şi reţele informaţionale. Teza a fost elaborată la Universitatea Tehnică a Moldovei.

Structura tezei. Teza conține Introducere, 3 capitole, concluzii generale și recomandări, bibliografia din 130 de titluri. Textul de bază constituie 117 de pagini, include 47 figuri, 23 tabele și 6 anexe. Rezultatele obținute ale tezei au fost publicate în 13 lucrări științifice.

Cuvinte cheie: Rețele definite prin software (SDN), OpenFlow, controller SDN, Hydra, rețea privată virtuală (VPN), Rivest-Shamir-Adleman (RSA), Blockchain.

Problemă de cercetare: creșterea nivelului de securitate a rețelelor de calculatoare folosind tehnologii bazate pe SDN.

Scopul cercetării este de a sublinia starea actuală de securitate a rețelelor de calculatoare și de a sugera noi soluții pentru a remedia diferite aspecte de securitate.

Obiectivele tezei includ analiza metodelor și tehnologiilor existente pentru asigurarea securității rețelelor de calculatoare, elaborarea algoritmilor și topologiilor pentru creșterea nivelului asigurării securității rețelelor de calculatoare și evaluarea eficienței topologiilor propuse pentru asigurarea securității rețelelor de calculatoare.

Noutatea științifică și originalitatea rezultatelor obținute sunt reflectate într-un cadru nou care asigură securitatea SDN și folosește diferite tehnici combinate pentru a face față punctului unic de eșec în arhitectura SDN, prevede un mecanism de apărare prin injectarea sursei de atac cu botnetele și utilizarea tehnicii de modelare a rețelelor Petri pentru a determina eficacitatea topologiilor propuse și a obține parametri de performanță, utilizați în ecuații bazate pe modelarea topologiilor specifice în ceea ce privește economisirea costurilor și descurajarea amenințărilor cibernetice precum atacurile DoS/DDoS.

Problema științifică importantă rezolvată constă în elaborarea unui nou set de algoritmi și topologii de controlere SDN pentru creșterea nivelului de securitate al SDN și elaborarea metodologiei de evaluare a nivelului de securitate al rețelelor de calculatoare.

Semnificația teoretică reflectă definirea principalelor probleme în asigurarea securității rețelelor de calculatoare, precizarea principalelor probleme din paradigma SDN care trebuie remediate, teoretizarea conceptelor esențiale ale algoritmilor și topologiilor propuse.

Valoarea aplicativă a lucrării este determinată de cadrul dezvoltat, care reprezintă o contribuție importantă pentru comunitatea SDN prin propunerea a câteva noi topologii SDN pentru a trata problema centralizării și protejarea conexiunii dintre mai multe controlere SDN. De asemenea, oferă o vizualizare mai bună a nivelului de securitate al unei anumite rețele prin măsurarea acesteia folosind diverse instrumente matematice care se bazează pe parametri propuși.

Implementarea rezultatelor. Rezultatele obținute au fost utilizate în investigațiile companiei Dekart privind noile abordări în domeniul securității informațiilor.

АННОТАЦИЯ

К докторской диссертации **«Обеспечение безопасности компьютерных сетей на основе программно-определяемых сетевых технологий»** представленной г-ном Али АМЕЕН на соискание ученой степени доктора наук в области Инженерных наук по специальности 232.01 – *Системы управления, вычислительная техника и информационные сети*. Диссертация была подготовлена в Техническом университете Молдовы.

Структура диссертации: Диссертация содержит введение, **3** главы, общие выводы и рекомендации, библиографию из **130** наименований. Основной текст составляет **117** страниц, включает **47** рисунков, **23** таблиц, и **6** приложений. Полученные результаты диссертации опубликованы в **13** научных работах.

Ключевые слова: программно-определяемые сети (SDN), OpenFlow, контроллер SDN, Hydra, виртуальная частная сеть (VPN), Rivest-Shamir-Adleman (RSA), криптовалюта, блокчейн.

Проблема исследовании: повышение уровня безопасности компьютерных сетей с использованием технологий на базе SDN.

Цель исследовании: определить текущее состояние безопасности компьютерных сетей и предложить новые решения для исправления различных аспектов безопасности.

Задачи диссертации включают в себя анализ существующих методов и технологий обеспечения безопасности компьютерных сетей, разработка алгоритмов и топологий для обеспечения безопасности компьютерных сетей и определение параметров оценки эффективности предлагаемых топологий обеспечения безопасности компьютерных сетей.

Научная новизна и оригинальность полученных результатов отражены в новой структуре, которая обеспечивает безопасность SDN и использует различные методы, объединенные вместе, чтобы справиться с единственной точкой отказа в архитектуре SDN, добавляет защитный механизм, вводя атакующий источник с ботнетами, использование метода моделирования сетей Петри для определения наилучшего результата предлагаемых топологий и получения различных параметров производительности, которые используются в уравнениях, основанных на этом моделировании этих конкретных топологий, чтобы определить производительность с учетом экономии затрат и сдерживания киберугроз, таких как DoS/DDoS-атаки.

Важной научной решаемой проблемой является разработка нового набора алгоритмов и топологий контроллеров SDN для повышения уровня безопасности SDN и разработка теоретической оценки уровня безопасности компьютерных сетей.

Теоретическая значимость может быть описана путем определения основных проблем в обеспечении безопасности компьютерных сетей, указания основных проблем в парадигме SDN, которые необходимо устранить, теоретизирования основных концепций предлагаемых алгоритмов и топологий.

Практическая ценность работы определяется разработанной структурой, которая представляет собой важный вклад в сообщество SDN, предлагая несколько новых топологий SDN для решения проблемы централизации и защиты соединения между контроллерами SDN. Также обеспечивается лучшая визуализация уровня безопасности конкретной сети путем измерения его с помощью различных математических инструментов, основанных на предлагаемых параметрах.

Внедрение результатов. Полученные результаты были использованы в исследованиях компании Dekart относительно новых подходов к информационной безопасности.

AMEEN ALI

SECURITY ASSURANCE OF THE COMPUTER NETWORKS BASED ON SOFTWARE DEFINED NETWORK TECHNOLOGIES

Summary of the Ph.D. thesis in Engineering Sciences

SPECIALTY 232.01 CONTROL SYSTEMS, COMPUTERS AND INFORMATION NETWORKS

Approved for printing: Paper size:
Offset paper: Type offset:
Print sheets: Order Number:

TUM, MD-2004, Chişinău, bd. Ştefan cel Mare şi Sfint, 168.
"Tehnica - UTM" Editorial Department
MD-2045, Chişinău, 9/9 Studenţilor str.