Intelligent Methods of Secure Routing in Software-Defined Networks

Olga Cherednichenko[1], Nataliia Sharonova[1], Ganna Pliekhova[2] and Nadiia Babkova[1]

[1] *Univ Lyon, Univ_Lyon 2, UR ERIC – 5 avenue Mendès France, 69676 Bron Cedex, France*
[2] *National Technical University «Kharkiv Polytechnic Institute», 2, Kyrpychova str., Kharkiv, 61002, Ukraine*
[3] *Kharkiv National Automobile and Highway University, 25, Yaroslava Mudrogo Str., Kharkiv, 61002, Ukraine*

Abstract

The object of research is the process of ensuring network security in Software-Defined Networks by routing means.
The subject of research is secure routing methods in Software-Defined Networks.
The work aims to research and improve existing methods of secure routing in Software-Defined Networks.
Research methods are analytical modeling, simulation, formalization, and comparison.
The work analyzes the standards, security, and vulnerabilities of Software-Defined Networks, as well as the CVSS standard for the quantitative calculation of network equipment's vulnerability level. Special attention is paid to analyzing the functionality of routing protocols as effective means of increasing network security in modern information and communication networks.
The mathematical model of secure routing has been improved, considering the base score of the vulnerabilities' criticality. The technological problem was formulated as an optimization problem with a quadratic objective function when the optimal route was chosen according to the combined metric under the base score of the vulnerabilities' criticality and the bandwidth of the network links that make up this route.

Keywords

Software Defined Network, network security, vulnerability, Common Vulnerability Scoring System, secure outing, modeling, intellect methods

1. Introduction

An intelligent system is one of the types of automated information systems that are based on knowledge. An intelligent system is a complex of software, linguistic, and logic-mathematical tools for the implementation of the main task: providing support for human activity and information search in an extended dialogue mode using natural language. The architecture of modern intelligent systems is based on knowledge bases that are formed according to the subject domain in which the intelligent system is used. The issue of researching intelligent software systems and organizing knowledge bases becomes relevant, especially decision support systems in various fields, including network security.

Presently, the implementation of network architectures, such as Software-Defined Networking (SDN), confronts emerging cybersecurity risks necessitating the formulation and examination of innovative specialized approaches to fortify network security [1-4]. Although SDN architecture offers heightened flexibility and adaptability, it supplants conventional networks while simultaneously raising the likelihood of various network intrusion attempts, thereby engendering fresh security predicaments.

The growing interest in SDN and wide deployment of various types of software-defined networks allow for the identification of their vulnerabilities in process of combating

COLINS-2024: 8th International Conference on Computational Linguistics and Intelligent Systems, April 12–13, 2024, Lviv, Ukraine
olga.cherednichenko@univ-lyon2.fr (O. Cherednichenko); nvsharonova@ukr.net (N. Sharonova); Plehovaanna11@gmail.com (G. Pliekhova); Nadjenna@gmail.com (N. Babkova)
0000-0002-9391-5220 (O. Cherednichenko); 0000-0002-8161-552X (N. Sharonova); 0000-0002-6912-6520 (G. Pliekhova); 0000-0002-2200-7794 (N. Babkova)

cybersecurity threats [4, 5]. It is obvious that security issues are closely related to characteristics of SDN networks themselves. In addition, security problems in SDN can be divided into three levels: data plane, control plane, and application plane.

At the same time, among the attack targets, there may be devices of different SDN levels. Therefore, according to the multilevel SDN architecture, security threats can be classified at the levels of data transmission, management, and applications. In turn, the data plane consists of switches and other network devices and is mainly responsible for data processing, forwarding, dropping, as well as collecting statistics. The operation of the data plane is based on flow rules provided by network controller. The main causes of security problems include the SDN architecture itself, external malicious attacks, insufficient access control, and encryption capabilities.

Today a significant role in the complex of network security measures, including SDN networks, is assigned to routing protocols that require systematic and coordinated interaction among multiple network elements simultaneously – SDN switches and network controllers – during formation (calculation) of paths and flow rules, along which the necessary level of security should be ensured according to selected indicators or criteria. An analysis of vulnerabilities in SDN data plane and functional capabilities of routing tools to counter potential attacks has demonstrated the prospect of using intelligent secure routing based on basic vulnerability criticality metrics to enhance the level of network security in SDN data plane. The analysis of CVSS standard for quantitative vulnerability assessment of network equipment justified its use in development and exploration of promising approaches to secure routing in the data plane of software-defined networks [5].

Thus, this work is dedicated to a relevant scientific-applied problem related to analysis of threats, attack targets, and improvement of potential solutions for enhancing level of network security in the data plane of SDN networks through the use of intelligent routing methods. The purpose of work is to research and improvement of existing methods of secure routing in software-defined networks using intelligent support tools.

2. Related works

A number of secure routing models have been developed and investigated, taking into account basic vulnerability criticality metrics. An existing model has been refined, leading to formulation of an optimization-based flow model for secure QoS routing (Figure 1). Numerical analysis has demonstrated the effectiveness and adequacy of proposed refinement.

Therefore, NFV consists of three main components [1]:

1. Virtualized Network Functions (VNF) are network functions implemented in software that can be deployed within a network function virtualization infrastructure (NFVI).
2. NFVI – common hardware and software components where they are deployed VNF.
3. Management and Orchestration Environment for NFV (MANO) is an architectural framework that includes functional blocks, data stores utilized by these blocks, and interfaces through which functional blocks exchange information for the management and orchestration of NFVI and VNF.

Key requirements and definitions regarding the security of NFV, SDN, and cloud technologies. To ensure the security of an object or system, there is a recognized need to provide five essential security functions – CIAAA [6-8]:

- Confidentiality;
- Integrity;
- Availability;
- Authenticity;
- Accountability.

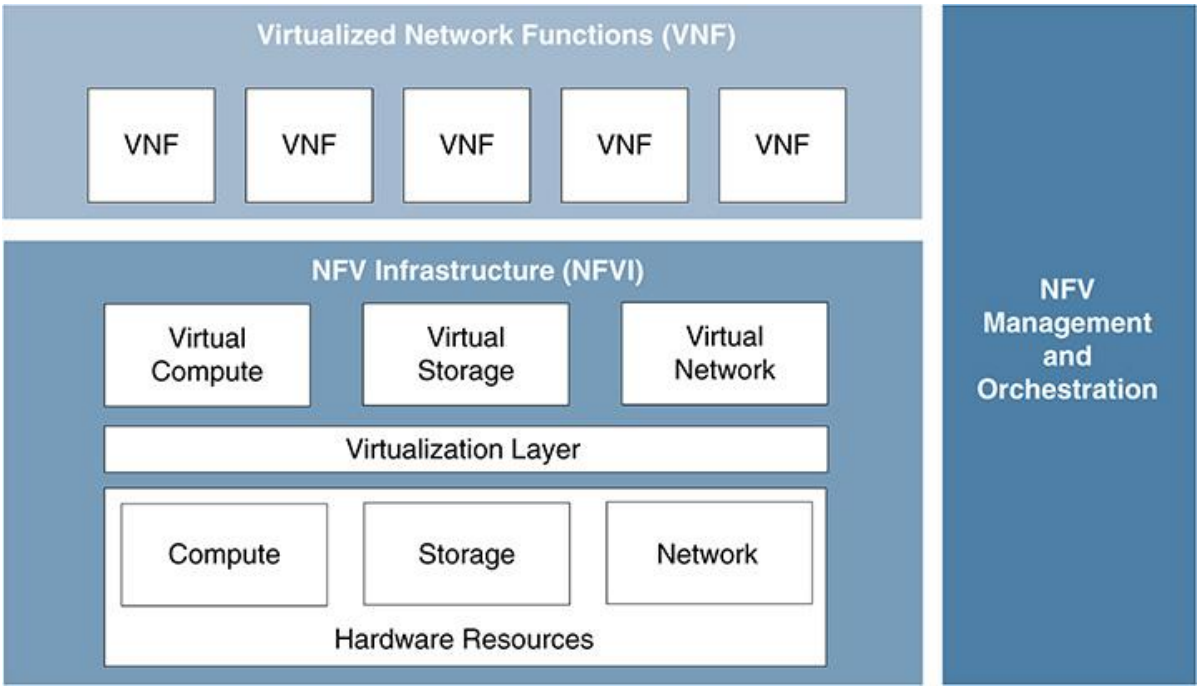

Figure 1: Concept of virtualization of network functions

So, confidentiality ensures the privacy and confidentiality of information about data or individuals and prevents its disclosure to unauthorized users. Integrity ensures that information and the expected operation of system will not be accidentally or intentionally altered by unauthorized users. Availability guarantees that unauthorized users cannot access systems and services. Authenticity ensures that users can be verified and trusted as who they claim to be, and that incoming data comes from a reliable source. Accountability generates the requirement for the actions of subject to be traced exclusively to that subject [6]. Each of these stages requires a convenient interface based on intelligent data processing, especially when presented in textual form.

A system, organization or cyberspace consists of three key elements:

- real and virtual objects (entities);
- interconnection (communications) infrastructure;
- interaction between objects through infrastructure.

Real and virtual entities encompass tangible objects and physical devices, such as people (users of system), computers, sensors, mobile phones, electronic devices and virtual abstractions of entities such as data/information, software and services. Infrastructure includes networks, databases, information systems and repositories that connect and support objects in system (space). Interaction, in turn, involves actions and interdependencies between objects in system (cyberspace) through interconnected infrastructure and information related to communication, policies, business and management [6].

Therefore, information or cybersecurity can be considered as systems, tools, processes, practices, concepts and strategies to prevent and protect cyberspace from unauthorized interaction by agents with elements of space to support and preserve the confidentiality, integrity, availability and other properties of the space and its resources that require protection.

Essentially, cybersecurity is related to identifying vulnerabilities in cyberspace, assessing the risks associated with threats exploiting these vulnerabilities and providing security solutions. Security vulnerability is a weak point in a system (component / product / system / cyberspace) that can allow an attacker to compromise the confidentiality, integrity, availability, authenticity or accountability of that system. Threats and risks are closely related but not equivalent. A threat is any entity, action or state that leads to harm, loss, damage, and / or deterioration of existing conditions. The risk associated with a threat is a characteristic that encompasses three components [6]:

- impact or significance of threat incident;
- probability or potential of a threat incident in future;
- potential losses (damages) due to a threat incident.

The risk assessment associated with a threat contributes to the development of new security solutions and formulation of requirements for these solutions [6-8].

3. Security issues NFV

As network components are virtualized, NFV networks include a level of abstraction that is absent in traditional networks. Securing this complex and dynamic environment, covering both virtual and physical resources, management elements, protocols, as well as the boundaries between virtual and physical networks, is a challenging task for several reasons according to CSA [6]. Among the main security issues are hypervisor dependencies: hypervisors are available from multiple vendors. They must address security vulnerabilities in controlled software. Understanding the underlying architecture, deploying appropriate encryption types and applying patches diligently are critical for hypervisor security. Another identified issue is elastic network boundaries: in NFV, network fabric performs numerous functions. The physical and virtual boundaries are blurred or absent in NFV architecture, complicating the design of security systems. Dynamic workloads present another challenge: while NFV offers flexibility and dynamic capabilities, traditional security models are static and cannot adapt when network topology changes according to requirements. Adding NFV services provides elastic, transparent networks, as fabric intelligently routes packets based on configurable criteria. Traditional security management elements are deployed logically and physically. In NFV, there is often a lack of a so-called security service insertion point that has not yet been placed on hypervisors. Stateful / stateless verification: Security operations over the past decade have been based on the assumption that stateful verification is more advanced than stateless. However, NFV can add complexity when security control mechanisms cannot handle asymmetric flows created by multiple duplicating network paths and devices. Another problem is scalability of available resources: deep inspection technologies, such as next-generation firewalls and TLS protocol decryption, require resources and do not always scale without offloading capability. ETSI security expert group, focusing on software architecture security, identified potential security vulnerabilities in NFV and determined whether they are new issues or existing problems in various forms and manifestations.

Security issues in SDN can be divided based on three levels: data plane, control plane, and application plane [6-8]. The data plane may suffer from various security threats, such as malicious OpenFlow switches, flow rule injection, "flooding" attacks (e.g., flooding the switch's flow table), forged or fake traffic flows, credential management and malicious hosts. The application plane inherits security issues such as unauthorized or unauthenticated programs, fraudulent role addition, lack of authentication methods and so on. The control plane faces several security issues related to centralized SDN controller, communication interfaces, policy enforcement, flow rule modification for packet modification, "flooding" communication between the controller and switch, security issues in SDN at system level (related to lack of audit accountability mechanisms), and lack of trust between the SDN controller and third-party applications. As control plane in SDN architecture acts as heart of this virtual network infrastructure, security vulnerabilities at this level can cause a failure in the entire virtual network architecture.

So, security threats related to SDN infrastructure are classified based on affected level (interface) as follows:

1. Application layer.
2. Management layer.
3. Data layer.
4. Application management interface.
5. Management interface.

From perspective of intelligence third and fourth levels draw maximum attention as knowledge bases can be created by shaping this knowledge from system text messages.

At the current stage of SDN architecture development, both domestic and foreign researchers believe that typical security problems in software-defined networks primarily manifest in aspects such as malicious software, controller vulnerabilities, legitimacy and consistency of flow rules, standardization problem of northbound interface and security in communication process using southbound interface, etc. Within the scope of this work, typical security problems and attack objects within the data plane – network devices controlled by SDN controller – are analyzed. The results of analysis are presented in Table 1. Clearly, devices at various network levels can be objects of attack and according to well-defined multilevel architecture of SDN, security threats can be classified at different levels. This work is dedicated to analysis of threats, attack objects and potential solutions to enhance level of network security in data plane of SDN networks through routing means.

Table 1
Typical security issues, attack targets and causes

Security Issue	Attack Target	Cause
Authorized Authentication	Network Equipment	Access Control
Legitimacy of Flow Rules	Flow Rules	Access Control
Consistency of Flow Rules	Flow Rules	SDN Architecture
DoS/DDoS Attacks	Flow Tables	SDN Architecture, Malicious Attack
Attack through third-party Channels	Data Privacy	Malicious Attack

The basic group of metrics represents internal vulnerability characteristics that remain constant over time and across users. It consists of three sets of indicators:

Exploitability: These indicators reflect ease and technical means by which a vulnerability is exploited. Indicators include:

- Attack vector, indicating how remote an attacker can be from vulnerable component.
- Attack complexity, conveying the level of complexity required by attacker to exploit vulnerability after identifying target component. Complexity is assessed as high if attacker cannot carry out attack at will but must exert effort for preparation or execution.
- Required privileges characterize access needed by attacker to exploit vulnerability. Values include "none" (privileged access is not required), "low" (basic user privileges) and "high" (administrator rights).
- User interaction indicates whether another user, apart from attacker, needs to participate for a successful attack.

Impact: These indicators indicate degree of impact on core security goals – confidentiality, integrity and availability. In each case, assessment reflects the worst result if more than one component is affected. For each of three goals, similar impact values are introduced: "high" (complete loss of confidentiality, integrity or availability), "low" (certain losses) and "none" (no impact).

Scope: This indicator is part of the basic metrics group, although it is somewhat independent of the rest of group. It relates to ability of a vulnerability in one software component to affect resources beyond its capabilities or privileges. An example is a vulnerability in a virtual machine allowing an attacker to delete files in the host operating system.

Usually, basic and temporal metrics are determined by vulnerability bulletin analysts, security software providers or vendors since they have better information about vulnerability characteristics than users. However, environment-related metrics are determined by users as they are best suited to assess the potential impact of a vulnerability in their own environment.

4. Analysis of SDN architecture vulnerabilities

Despite the numerous security challenges in cloud computing, Cloud Security Alliance has identified twelve critical security threats related to nature of shared on-demand cloud computing that have the greatest impact on corporate business:

1. Data Breach. A data breach is an incident during which confidential, protected or private information is disclosed, viewed, stolen or used by an unauthorized person.
2. Weak management of identity data, credentials and access. Data breaches and activation of attacks can occur due to lack of scalable identity data access management systems, non-use of multi-factor authentication, weak password usage and absence of automated cryptographic key, password and certificate rotation.
3. Unprotected Application Programming Interfaces (APIs). Provisioning, management, orchestration and monitoring are performed using a set of user interfaces or application programming interfaces. These interfaces must be developed with proper control to protect against both accidental and malicious attempts to bypass security policies.
4. System and Application Vulnerabilities. System vulnerabilities are errors in programs that can be exploited to infiltrate a computer system for data theft, system control or service disruption.
5. Stolen account credentials. This is a serious threat and cloud users should be aware of and guard against methods such as phishing, fraud and software vulnerabilities to prevent account data theft.
6. Malicious insiders. A current or former employee, contractor or other business partner with authorized access to an organization's network, systems or data, who intentionally abuses this access in a way that negatively impacts the CIAAA of the organization's information system, poses a malicious insider threat.
7. Advanced Persistent Threats (APTs). APTs are a parasitic form of cyber-attacks that infiltrate systems to establish themselves in the computing infrastructure of target companies, from which they steal data and intellectual property.
8. Data Loss. Data stored in the cloud may be lost not only due to malicious attacks. Accidental deletion by a cloud service provider or a physical disaster, such as fire or earthquake, can result in permanent data loss for the client.
9. Inadequate due diligence. An organization rushing to adopt cloud technologies and selecting cloud service providers without conducting proper due diligence exposes itself to numerous commercial, financial, technical, legal, and compliance risks.
10. Abuse and malicious use of cloud services. Poorly protected deployments of cloud services, free trial versions of cloud services, and fraudulent registration of accounts using payment fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks. Attackers may use cloud computing resources of users, organizations, or other cloud providers.
11. Denial of Service (DoS) Attacks. Denial-of-service attacks aim to interfere with users' access to their data or programs, forcing the target cloud service to consume an excessive amount of limited system resources, making service unable to respond to legitimate users.
12. Technology sharing issues. Cloud service providers deliver their services by sharing infrastructure, platforms, or applications. Infrastructure supporting the deployment of cloud services may not have been designed to provide robust isolation features for multi-tenant architectures (IaaS), redeployable platforms (PaaS), or multi-client applications (SaaS). This can lead to shared technological vulnerabilities that could potentially be exploited across all delivery models.

With the growing interest in Software-Defined Networking and widespread deployment of Software-Defined Networks, their vulnerabilities in combating cybersecurity threats are gradually becoming apparent. Security questions are closely related to characteristics of SDN.

According to research the following aspects make Software-Defined Networks vulnerable to attacks. Within the SDN architecture, separate levels are implemented for control plane and data plane, unlike traditional networks where these planes operate in a single device. The control plane formulates flow rules, while the data plane is responsible only for forwarding data packets according to flow rules.

For example, the lexicon used in such systems, which is fundamental for creating knowledge bases in intelligent systems, is provided in Table . This stage is necessary for forming a system of features to create logical equations.

Table 2
Values of Indicators for Calculating Basic Vulnerability Metrics of Network Elements

Loss of Confidentiality $Conf_i^q$		
Missing (M)	The possibility of compromising information confidentiality is absent	0,0
Partial (P)	There is a significant but limited disclosure of confidential information	0,275
Full (F)	There is complete disclosure of confidential information	0,66
Loss of Integrity Int_i^q		
Missing (M)	The possibility of compromising information integrity is absent	0,0
Partial (P)	There is a possibility of partial modification of data or system files	0,275
Full (F)	There is a possibility of modifying any data in node	0,66
Loss of Availability Av_i^q		
Missing (M)	The possibility of compromising resource availability is absent	0,0
Partial (P)	There is a possibility of reducing productivity or disabling some functions of the node	0,275
Full (F)	There is a possibility of a complete node failure	0,66

The specified indicators are basic metrics [10, 12] characterizing the overall complexity of implementing an attack using a particular vulnerability on the node of the network.

Representation and interpretation of knowledge play a crucial role in various fields of computer science. Different methods of discrete mathematics are used for formalizing information about objects and processes in knowledge bases. In cases where information about objects and processes is represented by discrete informational features and has a complex logical structure, various methods and models of discrete mathematics, including logical equations with Boolean variables, are used for its formal representation.

Logical classification methods typically involve the formulation and solution of logical equations with variables that take values of 1 and 0 depending on whether the object has a certain property or not. Solving such equations allows either identifying the object based on available sets of attribute variable values or determining the unknown properties of the object [15].

Logical classification methods for object categorization are applied to solving practical problems in various fields: biology, physics, meteorology, information security, etc. Their features can be revealed during the stage of constructing a mathematical model, taking into account specificities of data. Typically, propositional logic is used for this purpose. We propose an approach based on finite predicate algebra and method of comparison. The general form of such problems is built on basis of predicate equations.

Let the feature variables $y_1, y_2, \dots, y_l$ denote certain properties of objects, for example, the metrics values for calculating basic vulnerability metrics of network elements (Table). Each variable takes values from its domain. Unlike Boolean variables, predicate variables can take values from different domains.

Let discrete variables $x_1, x_2, \dots, x_n$ be features, by set of which we can determine possible values of property variables. Properties and features can be related to each other in the form of complex logical dependencies, which can be represented as predicate equations:

$$P(y_1, y_2, \dots, y_l;\ x_1, x_2, \dots, x_n) = 1, \quad (1)$$

where P is a finite predicate.

Classifying the considered object means determining, based on this predicate equation and experimental data about the features $x_1, x_2, \dots, x_n$ which properties (values of features $y_1, y_2, \dots, y_l$) this object has and which properties it does not correspond to [14, 15].

Then, based on the a priori dependency (1) and experimental data on the features $x_1, x_2, \dots, x_n$ it is possible to determine to which class the given object belongs. As evident from the above considerations, the values of features are grouped into a matrix.

Suppose that as a result of the experiment, we obtained some data related to values of features $x_1, x_2, \dots, x_n$ describing the classified object, and compiled the following predicate equation describing the relationships between them:

$$g(x_1, x_2, \dots, x_n) = 1. \quad (2)$$

The task of object classification can be formalized as solving the following predicate equation by finding the unknown predicate f:

$$g(x_1, x_2, \dots, x_n) \to f(y_1, y_2, \dots, y_l). \quad (3)$$

By solving this functional equation, one can determine the values of features $x_1, x_2, \dots, x_n$ that characterize objects $y_1, y_2, \dots, y_l$.

In research related to logical inferences in knowledge bases, questions arise about the tightness of relationships between the features of these objects, as well as questions about their significance or insignificance [14, 15]. It has been proven that the formal relationship between features is stronger the fewer sets of values of these variables satisfy the equation. In this case, if any sets of values of these variables satisfy the original equation, it can be considered that there is no connection between these variables.

A comparative analysis of existing models of secure routing, a QoS routing model with a metric analogous to the OSPF protocol, and an improved model of secure QoS routing taking into account basic vulnerability criticality metrics has been conducted. The study proved the adequacy and effectiveness of the proposed model, the feasibility of using intelligent methods for secure routing.

To solve the formulated optimization problem, a program was used, written in the Python language, using Python IDLE, Python GEKKO Optimization Suite, and NumPy.

5. Conclusions and further research

The article presents an important scientific and applied problem related to analysis of threats, attack objects and improvement of potential solutions to enhance level of network security in data plane of SDN networks using routing means with application of intelligent information processing methods and interface creation.

To achieve this goal standards for building software-defined networks were analyzed. It is noted that SDN is a modern approach to designing, building and operating information and communication networks by separating management and data forwarding planes. This distribution provides networks with direct programmability and dynamism as well as abstraction of functional capabilities from infrastructure layer. Network function virtualization has become a standardized way of developing, implementing and managing network services.

However, growing interest in SDN and their deployment has revealed their shortcomings in combating cybersecurity threats. At the current stage of SDN architecture development, it has been proven that typical security problems in software-configured networks primarily manifest

in aspects such as malicious software, controller vulnerability, legitimacy and consistency of flow rules, standardization issues of northbound interface and communication security during the use of southbound interface. Thus, main causes of security problems are SDN architecture itself, external malicious attacks, insufficient access control and encryption means. Based on research of typical security problems, it becomes apparent that centralized control and SDN programmability features provide powerful and convenient channels for attackers.

The analysis of vulnerabilities in SDN data plane and functional capabilities of routing means to counter possible attacks showed the prospect of using secure routing tools based on basic vulnerability criticality metrics to enhance the network security level of SDN data plane. In turn, the analysis of CVSS standard for quantitative vulnerability assessment of network equipment proved feasibility of its use in development and research of promising approaches to secure routing in field of intelligent data processing in software-configured networks.

The paper proposed improvements to existing secure routing model, taking into account basic vulnerability criticality metrics. Thus, routing metrics were modified so that resulting model would have properties of secure QoS routing. In improved model, the optimal route was selected considering both basic vulnerability criticality metrics and bandwidth of communication channels constituting this route. Additionally, model employed a quadratic optimality criterion for balanced distribution of flows transmitted in data plane of a software-configured network into substreams, taking into account chosen strategy of multi-path routing.

Acknowledgements

The research study depicted in this paper is funded by the French National Research Agency (ANR), project ANR-19-CE23-0005 BI4people (Business intelligence for the people)

References

[1] A. Sabella, R. Irons-Mclean, M. Yannuzzi, Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT, Cisco Press, 2018.

[2] J.F. Kurose, K. Ross, Computer Networking, 8th ed., Pearson, 2020.

[3] Pliekhova G., Sukhanova N., Lyubarskyi D. “Cyber security: threats, solutions”. Theoretical and scientific bases of actual tasks (2022), Lisbon, Portugal, pp. 656–660

[4] Pliekhova G.A., Kostikova M.V. “Actual problems of information security”. Modeling and information technologies in science, technology, cyber security and education 15.11(2022), Kharkiv, pp. 68–73. URL: https://rcf.khadi.kharkov.ua/fileadmin/F-HIGHWAY/Інформатики_і_ прикладної_ математики/ Матеріали_Всеукр.конф._2022_-1-ред.pdf

[5] Pliekhova G.A. “Analysis of routing tools to increase the level of network security in software-configured networks”. Problems of electromagnetic compatibility of promising wireless communication networks (EMS-2022), Kharkiv, KhNURE, pp. 41–42.

[6] Hoang, D.B., Farahmandian, S. “Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies”. In: Zhu, S., Scott-Hayward, S., Jacquin, L., Hill, R. (eds) Guide to Security in SDN and NFV. Computer Communications and Networks (2017). Springer, Cham. doi: 10.1007/978-3-319-64653-4_1

[7] Liu Y., Zhao B., Zhao P., Fan P., Liu H. “A survey: Typical security issues of software-defined networking”. China Communications (2019), volume 16(7), pp. 13–31. doi: 10.23919/JCC.2019.07.002

[8] Sagare A.A., Khondoker R. “Security Analysis of SDN Routing Applications”. In: Khondoker R. (eds) SDN and NFV Security. Lecture Notes in Networks and Systems (2018), volume 30, Springer, Cham, pp. 1–17. doi: 10.1007/978-3-319-71761-6_1

[9] Snihurov A., Chakrian V. “Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters”. Scholars Journal of Engineering and Technology (2015), volume 3 (8), pp. 707–714.
[10] Yevdokymenko M. O., Shapovalova A. S., Shapoval M. M. “Flow routing model taking into account information security risks using basic vulnerability criticality metrics”. Problems of telecommunications (2020), volume 1(26), pp. 48–62. URL: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf
[11] W. Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards, Addison-Wesley Professional, 2018.
[12] O.V. Lemeshko, O.S. Eremenko, M.O. Yevdokymenko, Modeling and optimization of safe and fault-tolerant routing processes in telecommunication networks, Kharkiv, KhNURE, 2022. doi: 10.30837/978-966-659-378-1
[13] Smelyakov K., Chupryna A., Sandrkin D., Kolisnyk M., "Search by Image Engine for Big Data Warehouse," IEEE Open Conference of Electrical, Electronic and Information Sciences (eStream-2020), Vilnius, Lithuania, pp. 1-4, doi: 10.1109/eStream50540.2020.9108782.
[14] Smelyakov K., Karachevtsev D., Kulemza D., Samoilenko Y., Patlan O., Chupryna A., "Effectiveness of Preprocessing Algorithms for Natural Language Processing Applications," IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T-2020), Kharkiv, Ukraine, pp. 187-191, doi: 10.1109/PICST51311.2020.9467919.
[15] Karataiev O., Sitnikov D., Sharonova N. “A Method for Investigating Links between Discrete Data Features in Knowledge Bases in the Form of Predicate Equations”, CEUR Workshop Proceedings (2023), Vol-3387, pp.224-235. URL: https://ceur-ws.org/Vol-3387/paper17.pdf