Critical Information Infrastructures Monitoring Based on Software-Defined Networks

Sergey Erokhin, Andrey Petukhov, Pavel Pilyugin
Moscow Technical University of Communications and Informatics, Moscow, Russia
esd@mtuci.ru, anpetukhov@yandex.ru, paul.pilyugin@gmail.ru

Abstract–**The paper deals with the problem of control of critical information infrastructures (CII) in order to ensure information security and functional reliability. It is proved that safety in such systems primarily affects the availability - that is, ensuring and maintaining the functionality and performance of all components of the CII. In second place is usually integrity, and the lowest priority is given to confidentiality. It is proposed to universalize monitoring information and telecommunication base of the CII. Software-defined networks (SDN) are considered as such base. Such monitoring will allow monitoring the state of the functionality of the information technology base of the CII objects and also to detect various violations of the functionality and anomalies in the operation of the information system and control systems. The monitoring protocols of traditional networks (NetFlow, sFlow) and SDN (OpenFlow) are compared. The analysis shows that the SDN switch can export NetFlow or sFlow data for later analysis. The scheme of the two-level sensor by means of the switch of the SDN and separate specialized devices is offered. It is assumed that these sensors can analyze parameters already for L2-L7 levels, such as DPI or DLP systems.Not only can the methodology and capabilities of IDS and IPS be used in the SDN, but based on the analysis of the data obtained, the network can be centrally reprogrammed to repel malicious attacks and restore functionality. This can make CII significantly more resistant to various failures, failures and malicious attacks.**

I. INTRODUCTION

With the increasing introduction of information and telecommunication technologies in all spheres of human activity, the task of ensuring the security of critical objects (CO) and providing them with critical information infrastructures (CII) becomes more and more urgent).

In 2011, the standard of information security of industrial control systems NIST SP 800-82 "Guide to Industrial Control Systems (ICS) Security"[1] appeared in the United States, and in the Russian Federation the Federal law 187 "On security of critical information infrastructure of the Russian Federation" dated 26.07.2017 was published[2].

These documents describe the concept of CII, contain recommendations for assessing the significance of CII objects and requirements for the information security system in CII.

Under the objects of the CII are understood objects operating in the fields of health, science, transport, communications, energy, banking, energy, nuclear energy, defense, mining, metallurgical, chemical industries, as well as telecommunication networks used to organize the interaction of such objects.

It should be noted that although initially information security had three objectives – confidentiality, accessibility and integrity. The strategy of providing information, typically allocated as the primary criterion of privacy, the second priority was the integrity, and the latter – accessibility.

In the context of CII, the priority of these tasks is changing. Since in this case the goals are pursued first of all:

- Ensuring the functioning of a significant object in the design modes of its operation under the influence of threats to information security;
- Providing the possibility to restore the functioning of a significant object of critical information infrastructure [3]

Thus, security in such systems primarily affects accessibility – that is, ensuring and maintaining the functionality and operability of all components of the CO. In second place is usually integrity, and the lowest priority is given to confidentiality. In certain circumstances, the integrity of the system may also have the highest priority, as it may directly affect the functionality of the CO.

It is important to note that in order to ensure functionality and operability, it is necessary not only to use an effective set of protection measures, but also to constantly monitor the functionality of the CII [4]. In essence, this feedback channel of the overall security management system of the CII. Indeed, in addition to incidents of information security violations, the CII may experience failures caused by shortcomings in the design of the system architecture, software and system component. The same disadvantages lead to vulnerabilities that can be used by attackers to violate information security [5].

The solution of control problems for the above application areas can be largely associated with the analysis of these subject areas and objects types used by the CII. As suchobjectscanact:

- Information system;
- Automated control system;
- Information and telecommunication networks.

At the same time, information systems and management systems are primarily related to the subject area, and the communication environment is more universal. This allows us to consider the creation of universal monitoring mechanisms for controlling objects of CII at the L2-L4 levels of the ISO/OSI model. This will allow to monitor the state of the functionality CII information base and also to detect various violations of the functionality and anomalies in the operation of the information system and control systems Thus, universal means of control of the communication environment can be an effective mechanism for detecting violations of the functionality of applied problems of various subject areas.

II. Information-telecommunication networks of CII and SDN

Functionally, the architecture of the information and telecommunication base of CII objects in general can be represented by several (at least three) levels:

- Transport layer;
- Level of transport management (switching);
- Level of service management (service and application).

The task of the transport layer is the transparent transfer of information to the CII user. As a rule, the basis of the transport level of the multiservice network of CII (for information systems and automated control systems) is supposed to use the existing packet data networks.

The task of the transport management layer is to process signaling information, route calls, and manage flows. The function of connection establishment is realized at the level of switches under external control of the equipment of the flexible controller of the alarm system. Alarm controllers can be placed in a separate hardware and software complex, designed to serve multiple switching nodes. In this case it is possible to consider two contours of telecommunication services: the communication infrastructure control loop (including routing of data streams) and the data transmission loop providing for delivery service provider data to consumers access points of this service.

One of the most suitable implementations of the stated of differentiation a control loop and a data transmission loop is the technology of software-defined networks (SDN). Basic SDN properties [6]:

- Separation of data transfer and management processes;
- A single and unified interface between the control level and the level of transmit data (for example, the OpenFlow Protocol);
- Logically centralized network management, performed by a controller with installed network operating system and implemented over network applications;
- Physical network resources virtualization.

In the context of the considered problem of control of CII, the most important SDN architecture characteristic is logically centralized management. A truly logically centralized but possibly physically distributed controller is the primary SDN component. To ensure the reliability of the components of the controller can be duplicated, but in the interest of consistency of centralized management is always defined as master and slave components (Master/Slave). The controller supports global network view and manages network devices based on network services policies.

This architecture allows you to organize and centralize monitoring, which is important not only for theSDNmanagement. Centralized monitoring in the SDN unifies infrastructure capabilities and creates a feedback loop with the controller to automate control functions in the network, usually this functionality can be combined in the controller. The controller-to-network interface based on the OpenFlow Protocol provides statistical and status information about the switch and its internal state (for example, the state of the flow maintained in the flow table, the state of ports and channels, statistical information about flows, ports, queues, and counters). These are all monitoring and control functions are part of the SDN architecture basic components. Based on this information, is possible to deploy network state visualization tools and solutions, such as sFlow, NetFlow, or integrate third-party functionality for network monitoring purposes. [7].

III. Traditional computer network and SDN monitoring protocols

Traditional networks consider data collection based on existing intrusion detection systems (IDS) and intrusion prevention systems (IPS). Special netflow and NetFlow monitoring protocols are used for this purpose.

NetFlow is a network protocol designed to account for network traffic developed by Cisco Systems. It is actually an industry standard and is not only supported by Cisco hardware. Based on this version, an open standard called IPFIX (Internet Protocol Flow information eXport, export of information about IP flows) was developed. The following components are required to collect information about NetFlow traffic:

Sensor. Collects statistics on the traffic passing through it. This is usually an L3-switch or router, although it can be stand-alone sensors.

Collector. Collects sensor data and puts it in storage.

Analyzer. Analyzes the data collected by the collector and generates reports (Solarwinds NTA or SolarWinds — Real-time NetFlow Analyzer).

The sensor, receiving IP packets, collects UDP or TCP stream parameters and sends them to the collector. The information collected in this way is generated in the collector record for each stream:

- The IP address of the source;
- Destination IP address;
- The source port for UDP and TCP;
- The destination port for UDP and TCP;
- Message type and code for ICMP;

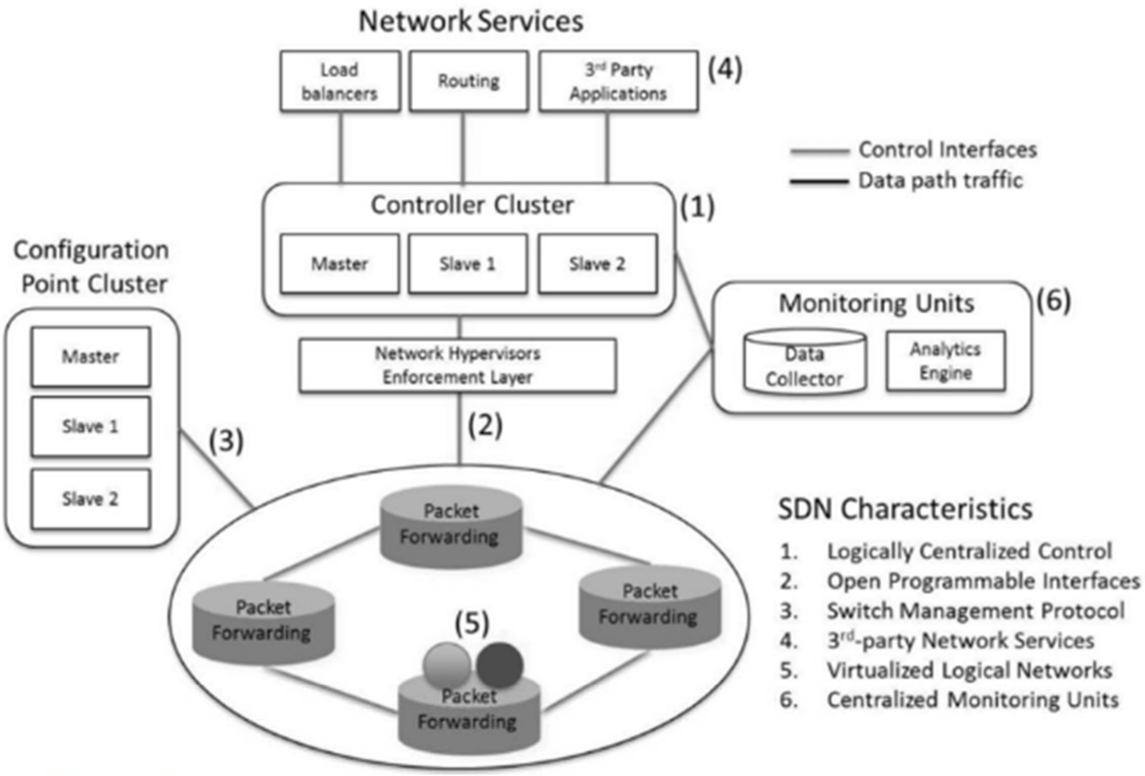

Fig.1. SDN architecture [7].

- Internet Protocol number of the transport layer encapsulated in the IP Protocol;
- Type of service (ToS);
- Network interface.

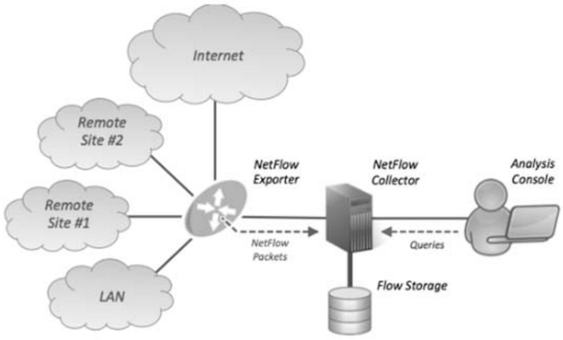

Fig.2. NetFlow architecture (https://en.wikipedia.org/wiki/NetFlow)

Depending on the Protocol version, the parameters may vary. Since the sensor is either a single host or a network device (router or switch), to analyze a large amount of NetFlow traffic include only some interfaces, or analyze not all, and every n-th packet, where n can be specified administratively or randomly (mode "sampled NetFlow"). Obviously, when using" sampled NetFlow", the resulting values are not accurate.

NetFlow and sFlow punctures are similar in many ways. Technology, sFlow uses sampling to obtain scalability.

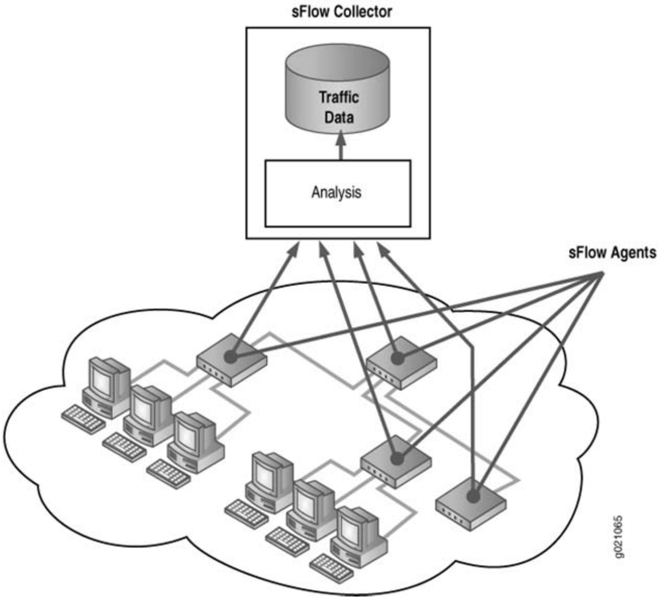

Fig.3. sFlow architecture (https://kb.juniper.net/InfoCenter/index?page=content&id=KB 14855)

The architecture of the sFlow system consists of a set of devices that provide two types of samples: random sampling of packets and operations at the application level and sampling at a certain time interval on the counter. The selected packet, operation, and counter data are sent as sFlow datagrams to the central server with an application that analyzes the traffic and generates the appropriate sFlow collector/analyzer reports. Multiple sFlow samples can be sent as a single datagram, and sFlow can be used by hardware or software.

A special communication protocol is used for interaction between the control plane and the data plane. The most common protocol OpenFlow, which is also available fields such as" source address"," destination"," source MAC-address"," Mac-address of the receiver"," port"," protocol " for effective management of data flows through the switches. And if traditional network sensors receive information from routing devices, then OpenFlow is a routing control protocol for creating flow tables in the switches and routers of the SDN. OpenFlow creates highly reliable high-speed networks with accurate transmission of packets to the desired receivers. At the same time, "skipping" of any packets as in NetFlow (sFlow) is impossible in the switch SDN, which makes it possible to more accurately examine the flows and control them.

However, the capabilities of the SDN-switch are not limited to data flow redirection, the switch functionality provides for the following actions in addition to forwarding the packet from the incoming port (s) to the outgoing port (s) [8]:

- Send fields of the packet to the controller (or whole packet: Packed in);
- Reset package;
- Packet buffering;
- Changing package fields;
- Sending counter data to the controller;
- Sending a packet to the network direction fromthecontroller (Packed out).

That is, the switch can export IPFIX, NetFlow, or sFlow data about flows, and the controller can export flows with network traffic details for later analysis.

Thus, the flexible architecture of the SDN and open software interfaces provide clear advantages in the development of network control capabilities. Not only can the methodology and capabilities of IDS and IPS be used in the SDN, but based on the analysis of the data obtained, the network can be centrally reprogrammed to repel malicious attacks and restore functionality. This can make the PCs significantly more resistant to various failures, failures and malicious attacks than traditional networks.

IV.THE CAPABILITIES OF PKS TO PROVIDE MORE COMPLETE MONITORING CUES

An effective anomaly detection and elimination system is built on the basis of combining OpenFlow and IDS - sFlow protocols [7]. The solution architecture describes three modules: (a) a collector in which the flow statistics are collected as far as possible using the OpenFlow and sFlow protocols, (b) anomaly detection in which the analysis is performed by statistics, and (c) anomaly mitigation. The combination of modules essentially acts as a network security feedback monitoring loop. It is possible to receive IDS/IPS data from both the controller and sensors. However, there is no need to place them in the node points of the network, as the necessary packets will be sent to the SDN by the switches according to the rules established by the controller.

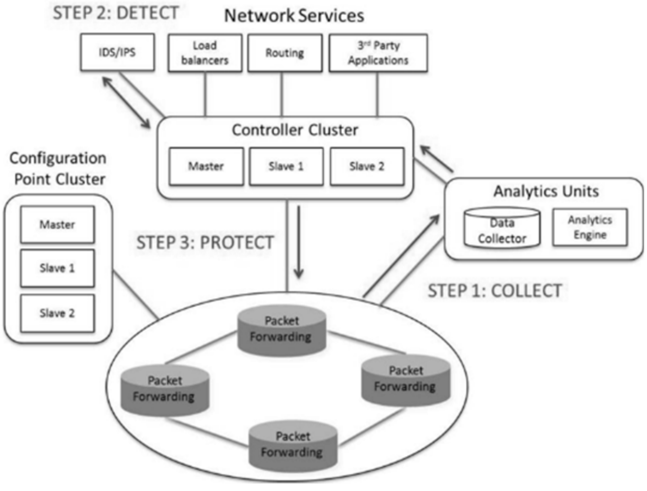

Fig.4. SDN security feedback control [7].

The proposed scheme, in fact, is a two-level sensor. At the first level of such a sensor, the L2-L4 level flow parameters are removed in the SDN switch and processed by the controller. As a result of such processing, the data, firstly, can be directed to further analysis, and, secondly, on the basis of their rules can be formulated to redirect certain flows to individual devices-sensors. Moreover, these sensors can be carried out analysis of parameters for L2-L7, for example systems DPI or DLP.

V. ACKNOWLEDGMENT

Various threats to different network planes were considered in the development of protection profiles of the main components of the SDN [6]. Profiles are a tool that allows you to determine the sequence of risk elimination in accordance with the objectives of the entire CII and its individual structural elements, taking into account the requirements of legislation, regulators and best practices, as well as reflecting the priorities of the safety management process.

As part of the profiles were defined as the purpose of protection of the network components, and the purpose of the environment, that is, what should resist the environment. Together, they should describe harmonized in the sense of General criteria for the threat of the SDN [6]. The analysis of possible threats to the CII security [5] and the assessment of the possibility to counteract them by the methods described above allow specifying the tasks of CII control to ensure information and functional security. Note that in CII, as in the SDN, the most important tasks are to ensure the availability and integrity of information.

As actual threats, the SDN were considered in accordance with the STRIDE method [9]: (Spoofing) attacks on the network configuration, (Tampering) attack as a result of NSD, (Information Disclosure) data leakage, (Dos) denial of service, data modification (Elevation of privilege). All of the attacks described had the ultimate goal of disrupting the functionality of various components of the network.

Development of methods of counteraction to these threats occurs in three directions [9]:

- Development of means fortraditional networkingprotection;
- Development of tools based on the use of SDN capabilities;
- Creation of new means for SDN architectureprotection.

If we do not consider such, of course, the most important means of authentication and crystallographic protection, not related to the topic, all other basic security mechanisms are based on the control of flows and network topology (firewall, IDS/IPS). The emphasis is placed on the use of new features of the SDN (for example, methods of load balancing, combining and mirroring streams, sensing packages Packed out) and additional devices. As shown by the research [7], the use of SDN now allows not only to detect, but effectively to reflect many denial of service attacks and to deal with overloads and failures of network components. The basis of all these methods is the system of analysis of information flows, network topology and network equipment. And if the considered methods of control allow not only to collect, but also to manage the collection of necessary information, the development of algorithms for the analysis of this information is not an easy task [9].

References

[1] NIST Special Publication 800-82 Revision 2 «Guide to Industrial Control Systems (ICS) Security», May 2015. 247 c.

[2] The Federal law 187 "On security of critical information infrastructure of the Russian Federation" dated 26.07.2017

[3] The Order of FSTEC of Russia No. 239 of 25.12.2017 "About the approval of Requirements to safety of significant objects of critical information infrastructure of the Russian Federation" (it is Registered in the Ministry of justice of Russia 26.03.2018). 28 p.

[4] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration — Part 1: Models and Terminology

[5] Andrey Petukhov, Pavel Pilyugin, Karina Pilyugina. Harmonization of critical information infrostructure objects threats. International conference "Technology&Entrepreneurship TEDS 2018", Moscow, 2018

[6] Andrey Mukhanov, Andrey Petukhov, Pavel Pilyugin. «Common criteria and software defined networks (SDN) security». International sciense and tecnology conference "Modern network technologies", MoNeTec-2018, Moscow, 2018 http://www.arccn.ru/media/monetec_final/

[7] Scott-Hayward, S., Natarajan, S., & Sezer, S. «A Survey of Security in Software Defined Networks». IEEE Communications Surveys and Tutorials, (2016) 18(1), pp 623-654. https://doi.org/10.1109/COMST.2015.2453114

[8] Arash Shaghaghi, Sanjay Jha, Mohamed Ali Kaafar, Rajkumar Buyya. «Software-Defined Network (SDN) Data Plane Security:Issues, Solutions and Future Directions» Article · April 2018 https://www.researchgate.net/publication/324167015

[9] Shang Gao, Zecheng Li, Bin Xiao, Guiyi Wei. «Security Threats in the Data Plane of Software-Defined Networks» *IEEE Network* , Volume 32, pp 108-113; doi:10.1109/mnet.2018.1700283