UDC 519.218.31

Minimum Architecture of SDN Tolerant to Failure of a Switch

Alexander A. Grusho, Elena E. Timonina, Sergey Ya. Shorgin

[*] *Institute of Informatics Problems, Federal Research Center*
"Computer Science and Control" of the Russian Academy of Sciences
44-2 Vavilova st., Moscow, 119333, Russian Federation

Email: grusho@yandex.ru, eltimone@yandex.ru, sshorgin@ipiran.ru

Fault tolerance to a switch in SDN (Software Defined Network) requires implementation of redundancy. The article is devoted to research of some economical methods of entering of redundancy into SDN which allow to provide stability to failure of one switch. We will apply the method both to peer-to-peer networks, and to hierarchically organized peer-to-peer networks.

It is proved that the constructed peer-to-peer SDN architecture concerning the number of switches is minimal. It is shown how to generalize results for a simple peer-to-peer network to a set of peer-to-peer networks.

Key words and phrases: Software Defined Network; fault tolerance; information security; network architecture.

In: K. E. Samouylov, L. A. Sevastianov, D. S. Kulyabov (eds.): Selected Papers of the 12th International Workshop on Applied Problems in Theory of Probabilities and Mathematical Statistics (Summer Session) in the framework of the Conference "Information and Telecommunication Technologies and Mathematical Modeling of High-Tech Systems", Lisbon, Portugal, October 22–27, 2018, published at http://ceur-ws.org

1. Introduction

Security facilities of SDN (Software Defined network) [1], [2], shall prevent a loss of information and network resources. Traditionally losses of resources are estimated with use of probability models [3], [4], [5]. The choice of network architecture is able to reduce or to get rid absolutely of losses [6], [7], [8], [9], [10].

Fault tolerance to a switch in SDN requires implementation of redundancy. The article is devoted to research of some economical methods of entering of redundancy into SDN which allow to provide tolerance to a failure of one switch.

The main idea of approach consists in organizing redundancy in the simplest case of a peer-to-peer network. It is obvious that the simpler elementary construction component is arranged, then more architectural structures can be constructed on its basis. In the paper simplest peer-to-peer SDN is defined, and it is proved the minimality of its design. Further, using this design as a construction component, it is possible to construct various more complex architecture of SDN. This principle of construction is based on the idea of self-similar structures.

Any network can be decomposed into a system of interacting peer-to-peer networks.

2. Structure of SDN

Usually SDN is presented in the form of three planes. The plane of data (Data Flow Level) consists of hosts and switches. Each switch has Flow table (FT). In this table there are rules for the switch for forwarding data. The order of number of such rules can be more 1000. Rules of the table contain several fields:

– action;
– counter;
– example.

The packet arriving on the switch is being processed as follows. The switch looks for data in FT, after finding of the rule the counter increases its value, and there is an action intended for such packet. If the rule isn't found, then the packet header comes to the controller or the packet is discarded at all.

Rules are created by the controller. The plane of the controller is described as follows. Host of the controller is connected to switches either via the common channel, or via the special channel. The controller creates routes for connection of hosts. On the third plane there are applications which support the functions of the controller.

From the information security point of view an usage of hosts for the organization of connections at a network isn't always secure. So, the malicious code can be the initiator of a connection. Therefore on a network it is necessary to use special rules to provide restrictions for information flows. Such rules may be installed into FT and can be deleted when the necessity disappears. This method of dynamic flow control can be organized by meta data [11] and other security features. If interactions of hosts are defined only by necessary interactions, then problems with information security become less. The controller has task of formation of routes for interaction of legal tasks, or subnets.

Let's consider SDN which creates a peer-to-peer network of communication of n hosts of $X = \{x_1, ..., x_n\}$. SDN is defined by the controller of y_0 and switches of $Y = \{y_1, ..., y_m\}$. Each switch possesses a set of k ports. We will assume that all switches are identical, and everyone has the minimum number $k = 3$ of ports. If $k = 2$, then the switch is the packet filter which is not participating in formation of a network.

The architecture of a network is defined by the organization of interactions of switches, controllers and hosts [12]. The necessary condition on the peer-to-peer network is the possibility of connection of each host with each host.

3. Architecture of the complete tree

Let's consider the simplest case when all switches form a complete rooted 2-tree. The tree root through one of ports is connected to the controller. If at all switches all ports are used, then such tree can provide communication with $n = 2^h$ hosts where h is height of 2-tree. Number of switches in such tree is $m = 2^{h-1}$, in the maximum case is $m = n - 1$. If $n \leq 2^h$, then in this architecture of a network some ports are not used, and can be that some switches are not used.

We will mark shortcomings of this architecture.

1. In this architecture there is no resistance of a network to failure of one switch. In case of failure of one switch, at least, two hosts are not achievable.
2. If the faulty switch is close to the root of the tree of the network of switches, then all switches and hosts on the descending branches of this tree are unattainable.
3. In case of failure of the rooted switch the controller becomes unavailable that does not allow to build new routes in architecture of the complete tree.

4. The architecture of SDN allowing functioning in case of failure of one switch

Let's sequentially build an architecture of SDN which allows a stability of communication in case of failure of one switch. At the same time the problem consists in that the number of switches should be minimal. The simplest case solving the problem of stability of a network of switches in case of possible loss of one host is provided in Figure 1. Hereinafter the controller is designated by a square, the switches – by circles, the hosts – by points, and all communications are designated by lines.

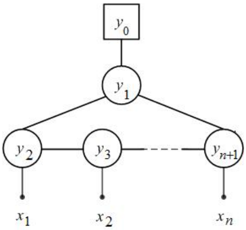

Figure 1. Architecture of protection against failure of a switch with possible loss of one host.

In this architecture of $n + 1$ of switches all $3(n + 1)$ of ports of switches are also used. Unlike a complete tree the number of switches is connected to number of hosts.

Theorem 1. *The architecture of a network (see Figure 1) is tolerant to a failure of one of switches with possible loss only of one host, and is minimum of number of switches.*

Proof. We will consider architecture of the network provided in Figure 1. This architecture is tolerant against failure of one switch from the set of $(y_2, ..., y_{n+1})$ switches, though at the same time access to one host is lost, i.e. in case of failure of the switch y_i the host x_{i-1} remains unavailable. Really, if there was a failure of the switch y_i, $i = 2, ..., n + 1$, then usage of FT when the port to switch y_2 has input from the switch y_1, allows to transfer information to all working switches which are to the left of the faulty switch. Similarly, when the port to the switch y_{n+1} has input from the switch y_1, information can be transferred to all working switches which are to the right of the faulty switch, and the direction of an information flow is defined by the controller.

Failure of the switch y_1 separates remaining switches from the controller. At the same time formally the communication system on the peer-to-peer network of hosts can function out of the connection with the controller since all FT of the remained switches allow to organize a peer-to-peer network.

The provided architecture is minimal on the number of switches with the properties described above. In this case the architecture of a network is organized by means of $n+1$ of switches.

We will assume that there is an architecture of SDN with number $m \leq n$ of the switches which is tolerant to a failure of only one switch, and at the same time one host can be lost. Total number of ports at all switches is equal to $3m \leq 3n$. At least one port of the switch y_1 shall connect the network of switches to the controller. There is $3m-1$ of ports. Let n of ports be used for communication with each of hosts. It means that in case of loss of some switch, at least, communication with one host can be lost. There is $3m-n-1$ of ports.

Resistance to failure of one switch when maintaining connectivity is provided that each switch is located on a simple cycle [13], [14]. The minimum number of edges contains in a full cycle, and the number of edges in a full cycle is equal to m. It follows from this that for implementation of m of edges it is necessary $2m$ of ports. From here in case of $m \leq n$ the number of ports is negative, therefore, the contradiction to the assumption is received. Thus, the minimality of this diagram is proved. The theorem 1 is proved.

When it is necessary to guarantee communication of switches in peer-to-peer network with the controller, it is necessary to carry out duplication, i.e. instead of one switch y_1 to install two switches of y_1' and y_1'' (Figure 2).

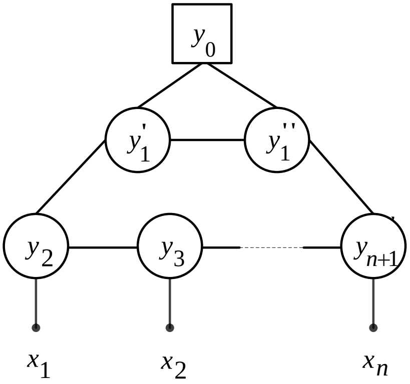

Figure 2. Architecture of protection against failure of a switch with possible loss of one host.

Theorem 2. *The architecture of a network* (see Figure 2) *is tolerant to failure of one of switches with possible loss only of one host and necessary connection with the controller and has minimum number of switches.*

Proof. As well as in case of the theorem 1, architecture of Figure 2 is tolerant against failure of one switch since all switches are on a simple cycle and the connection with the controller always exists. The minimality of architecture follows from the fact that all ports are used and the entered additional switch guarantees interaction with the controller of the network. The theorem 2 is proved.

In certain cases there is a need to duplicate the SDN controller for increasing a reliability of its functioning. In the considered conditions the only minimum solution of such duplication is the scheme on Figure 3 (see Figure 3) where y' and y'' are the switches realizing interaction of the main and reserve controllers.

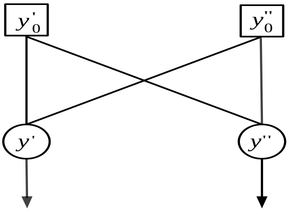

Figure 3. Minimal architecture for implementation of additional controller.

It follows from the fact that usage of one switch for communication of two controllers will not allow implementation of connections with controllers at failure of the only switch.

From Figure 3 it follows that the direct connection of remained ports with switches y_2, ..., y_{n+1} of peer-to-peer network will not allow to provide resistance to failure of one switch. It follows from the fact that connection of switches y' and y'' with switches y_2, ..., y_{n+1} does not form a cycle. From this it follows that introduction of the reserve controller will demand realization of the architecture on Figure 2 with only that difference that y_1' connects to y', and y_1'' connects to y'' (see Figure 4). It is possible to prove that the received scheme is minimum.

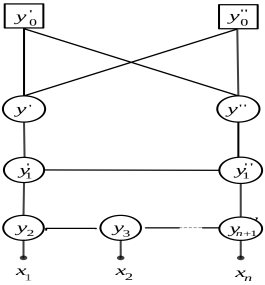

Figure 4. Minimal architecture with reserved controller.

Communication with other networks cannot be carried out in this architecture. It supports requirements for security of interaction between networks.

Little changes of these diagrams allow to get rid of danger switch-off of the host x_{i-1}, $i = 2, ..., n+1$, in case of failure of the switch y_i.

If to allow $k = 4$, then shortcomings of a complete 3-tree remain. But in the considered diagram it is possible to get rid of loss of a host. It is reached by means of additional connection of switches with hosts (see Figure 5).

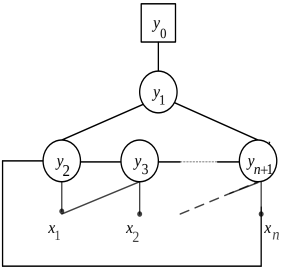

Figure 5. Architecture of protection in case of failure of the switch without loss of a host in case of $k = 4$.

The protection from loss of a host in case of one failure of a switch follows from the fact that each host and each switch lie on a simple cycle. At the same time resistance to a failure of system follows from [13], [14].

It is possible to avoid loss of a host in case $k = 3$ by means of duplicating of a chain of switches (Figure 6).

The protection from loss of a host in case of one failure of a switch as well as in the previous case follows from the fact that each host and each switch lie on a simple cycle. At the same time resistance to failure of system follows from [13], [14].

5. Self-similar architectures with P2P SDN

We will assume that the set of hosts is divided into s not crossed peer-to-peer networks. It is equivalent to existence of function $f : X \to Z$, where $Z = \{z_1, z_2, ..., z_s\}$ is a set of identifiers of peer-to-peer networks.

The diagram provided in Figure 7 is built according to the principle of a fractal due to repetition of the diagram in Figure 2 of a set of peer-to-peer networks. At this diagram resistance to loss of a host is not considered, however a resistance to failure of one switch follows from the fact that all switches are located on simple cycles.

In considered diagrams a connection with the controller is necessary and therefore duplicating of the switch connecting the network to the controller is used. In this diagram it is assumed that information of isolated peer-to-peer networks can securely be transmitted through switches of higher levels.

System of peer-to-peer networks can hierarchically be build, for example, one of such networks can be a master and can control information flows between other peer-to-peer networks. In this case the model of control of admissible flows represents meta data which the controller uses for entering of special tags into FT of switches. Such decision

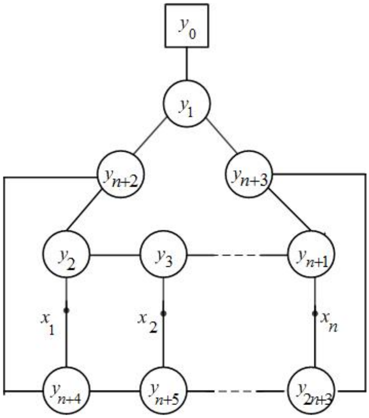

Figure 6. Architecture of protection in case of failure of one switch without loss of the host in case of $k = 3$.

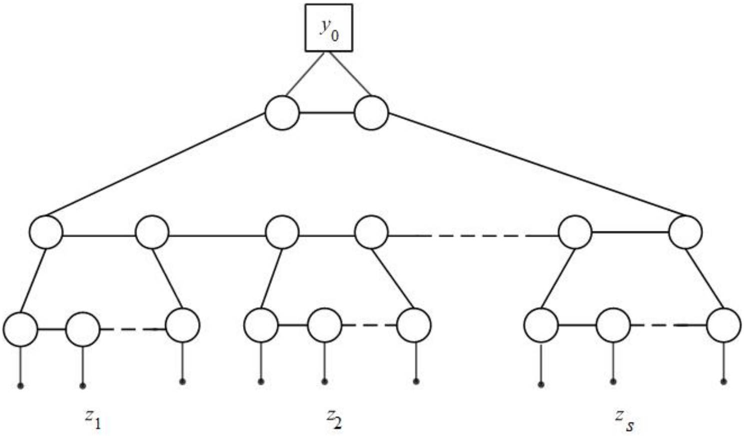

Figure 7. Architecture of protection of a system of several peer-to-peer networks in SDN.

is possible because there is a channel from the master peer-to-peer network to the third SDN through y_0.

Another architecture can be build on the basis of diagram in Figure 2. Let's consider a question of connection of several SDN. Let for simplicity the number s of peer-to-peer

SDN be equal to 3. Let each peer-to-peer network be minimum with a guarantee of access to the controller (see Figure 2). Then the simplest scheme of integration of these networks is submitted in Figure 8.

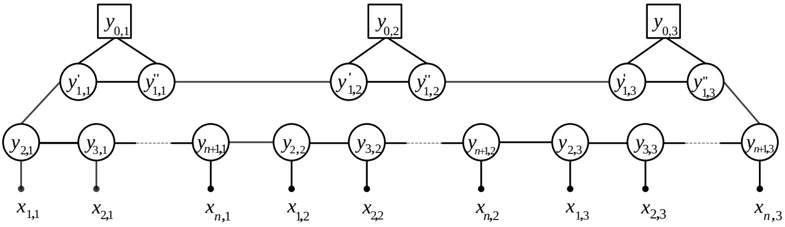

Figure 8. The simplest architecture of peer-to-peer SDN union.

Architectures of SDN in Figure 2 and Figure 8 assume that components of network are not remote far from each other.

However at connection of several peer-to-peer SDN there can be a requirement of use of the main channels connecting them. In this case the architecture of each networks has to have a possibility of independent functioning or functioning as a part of the associations of SDN. The architecture of such decision demands introduction of additional redundancy which is presented in Figure 9 where the fat line designated the main communication channel. Additional redundancy is achieved by additional switches.

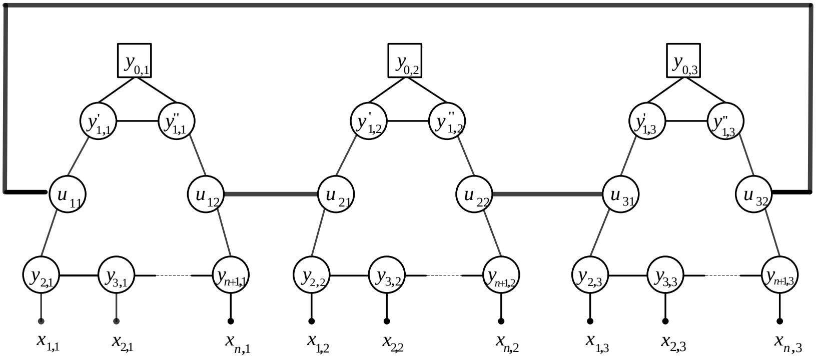

Figure 9. Union of remote SDN.

6. Conclusion

In the paper the architectures of SDN allowing to protect communication of all working switches for a peer-to-peer network are constructed. It is proved that the architecture of creation for switches with the minimum number $k = 3$ of ports is minimal on a number of used switches. The shortcoming of the constructed minimum architecture is that in case of failure of the switch there can be an unavailability of one host.

It is possible to correct this shortcoming or by means of increasing in number of ports in switches to $k = 4$, or by means of increasing in number of switches in case of $k = 3$. The constructed architecture can be generalized on a set of the peer-to-peer networks working under one controller.

By means of the organization of the additional channel to the third SDN level it is possible to construct the hierarchical system of peer-to-peer networks.

The usage of the idea of the simple P2P SDN (Figure 2) it is possible to construct a union of several SDN. It is even possible when connection demands main channels.

Acknowledgments

The reported study was supported by the Russian Science Foundation, research project No. 16-11-10227.

References

1. Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, M. Imran, Security in Software-Defined Networking: Threats and Countermeasures. J. Mobile Netw. Appl. **21** (5) (2016) 764–776.
2. A. Grusho, N. Grusho, V. Piskovski, E. Timonina, Five SDN-oriented directions in information security. SDN and NFV: The Next Generation of Computational Infrastructure: 2014 International Science and Technology Conference Modern Networking Technologies (MoNeTec). (2014) 68–71.
3. V. Naumov, K. Samouylov, Analysis of multi-resource loss system with state-dependent arrival and service rates. Probability in the Engineering and Informational Sciences **31** (4) (2017) 413–419.
4. A. Samuylov, D. Moltchanov, Y. Gaidamaka, S. Andreev, Y. Koucheryavy, Random Triangle: A Baseline Model for Interference Analysis in Heterogeneous Networks IEEE Transactions on Vehicular Technology **65** (8), (2016) art. no. 7275184, 6778–6782.
5. B. Xiong, K. Yang, J. Zhao, W. Li, K. Li, Performance Evaluation of OpenFlow-based Software-defined Networks Based on Queuing Model. Comput. Netw. **102** (2016) 174–183
6. A. A. Grusho, N. A. Grusho, E. E. Timonina, Security evaluation in secure architecture of distributed information systems. Systems and Means of Informatics **26** (4) (2016) 31–37.
7. A. A. Grusho, N. A. Grusho, E. E. Timonina, S. Ya. Shorgin, Possibilities of secure architecture creation for dynamically changing information systems. Systems and Means of Informatics **25** (3) (2015) 78–93.
8. A. A. Grusho, N. A. Grusho, E. E. Timonina, Information Security Architecture Synthesis in Distributed Information Computation Systems. Automatic Control and Computer Sciences,. **51** (8) (2017) 799–804.
9. N. A. Grusho, V. V. Senchilo, Modeling of secure architecture of distributed information systems on the basis of integrated virtualization. Systems and Means of Informatics **28** (1) (2018) 110–122.
10. A. T. Nguyen, T. Eom, S. An, J. S. Park, J. B. Hong, D. S. Dan Kim, Availability Modeling and Analysis for Software Defined Networks. The 21st IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2015) 159–168.

11. A. Grusho, N. Grusho, M. Zabezhailo, A. Zatsarinny, E. Timonina, Information Security of SDN on the Basis of Meta Data. In: Rak J., Bay J., Kotenko I., Popyack L., Skormin V., Szczypiorski K. (eds) Computer Network Security. MMM-ACNS 2017. Lecture Notes in Computer Science **10446** (2017) 339–347.
12. G. Pantuza, F. Sampaio, L. Viera, D. Guedes, M. Viera, Network Management through Graphs in Software Defined Network. 10th CNSM and Workshop, IFIP (2014) 400–405.
13. F. Harary, Graph Theory. Addison-Wesley, Reading, MA (1969) 214 p.
14. O. Ore, Theory of graphs. American Mathematical Society (1962) 279 p. 77–79.