THE OVERVIEW OF CYBER RESILIENCE APPROACH USING TRAFFIC ENGINEERING FAST REROUTE FEATURES

O. Yeremenko, A. Mersni, A. Akulynichev
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
oleksandra.yeremenko.ua@ieee.org, amal.mersni.ua@ieee.org, artem.akulynichev@nure.ua

The research is dedicated to evaluating and developing a method for assuring cyber resilience based on Traffic Engineering Fast ReRoute with the assistance of Traffic Policing mechanism. The suggested approach is founded on a mathematical model defined by multipath routing conditions and modified flow conservation conditions. Additionally, it considers traffic policing at the network edge and conditions for protecting (reserving) the link, node, and network bandwidth, all of which are tailored to meet cyber resilience needs. The proposed solution has the advantage of recasting the problem as a linear optimization. The numerical example demonstrates the model's operability and the adequacy of the findings acquired using it.

Modern communication networks demand technological solutions to provide cyber resilience against network attacks, compromises, etc. Only the suitable reserve capacity can identify these repercussions [1-5]. When compromising a network element, such as a link, a node, or even an entire network segment, a network reserve with sufficient bandwidth is necessary.

Assuring a network's cyber resilience is a difficult task. The study reveals that using Fast ReRouting (FRR) effectively can improve the network's cyber resilience [5-8]. The network can respond operationally (in tens of milliseconds) to possible service issues. However, this requires resource redundancy, as well as rapid computation and the use of backup routes. Such routes do not share a network element with the main working path. However, enhancing the cyber resilience of an infocommunication network via resource reservation always has a detrimental effect on the overall Quality of Service (QoS) level [9-10]. Consequently, strengthening the cyber resilience of an infocommunication network by reserving network resources inevitably reduces overall QoS. This is especially true when the network's resources, notably bandwidth, are insufficient to perform a particular protective system that may cause network overload.

Thus, to avoid network congestion induced by applying cyber resilience principles, two things must be ensured during Fast ReRouting [11, 12]. Firstly, the balanced use of available network resources on the Traffic Engineering principles should be implemented. Secondly, priorities of limiting (policing) traffic at the network edge may be applied.

Therefore, the pertinent scientific and practical task is developing of novel approaches for ensuring the cyber resilience of communication networks following the requirements for network resilience, security, and QoS when using traffic management technologies such as Traffic Engineering and Traffic Policing in conjunction with the means of Fast ReRouting in the event of a network element failure.

In modeling the cyber resilience strategy based on Traffic Engineering Fast ReRoute, the network structure is represented by a graph. The nodes of the graph are network routers, and the communication links connecting these routers are edges. The presented approach is based on a mathematical model that incorporates conditions for multipath routing, updated flow conservation conditions that account for network edge Traffic Policing, and link, node, and network bandwidth protection (reservation) conditions. The advantage of the suggested method is that it recasts the Traffic Engineering Fast ReRoute under the Traffic Policing (TE-FRR-TP) task as an optimization problem. The optimality criterion is defined as the minimum of a linear function that sums the use of dynamically managed upper bound of network links utilization under the Traffic Engineering requirements. The linearity of the formulated optimization problem is intended to reduce the computational complexity associated with calculating the routing variables that determine the primary and backup paths.

The work proposes a cyber resilience approach based on Traffic Engineering Fast ReRoute with policing. The study's results on various numerical network topologies supported the proposed cyber resilience approach's efficacy and suitability. It is worth noting that providing cyber resilience necessitates the involvement of extra network resources, both topological (links, nodes) and

functional (bandwidth of network elements). Thus, the innovation and primary benefits of the proposed approach are as follows. First, it is advocated to coordinate the effective (balanced) usage of network resources according to the TE-FRR principles to avoid network overload while ensuring cyber resilience. Second, it is proposed to implement Traffic Policing at the network edge, both in primary and backup routes, prioritizing the flows into account. The developed model is a continuation and improvement of previously known approaches to load balancing during Fast ReRouting [12] and traffic policing [13].

Keywords: Cyber Resilience, Traffic Engineering, Fast ReRoute, Traffic Policing, Bandwidth Protection.

References

1. Linkov I., Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In Cyber resilience of systems and networks (pp. 1-25). Springer, Cham.
2. Stallings W., Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional, 2018.
3. Galinec D., Steingartner W., Combining cybersecurity and cyber defense to achieve cyber resilience, in Proc. 2017 IEEE 14th International Scientific Conference on Informatics, November 2017, pp. 87-93.
4. Björck F., Henkel M., Stirna J., Zdravkovic J., Cyber resilience–fundamentals for a definition. New contributions in information systems and technologies, Springer, Cham, 2015, pp. 311-316.
5. White M.B. Computer Networking: The Complete Guide to Understanding Wireless Technology, Network Security, Computer Architecture and Communications Systems (Including Cisco, CCNA and CCENT). CreateSpace Independent Publishing Platform, 2018.
6. Monge A.S., Szarkowicz K.G. MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services. O'Reilly Media, 2016.
7. Al-shawi M., Laurent A. Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide: CCDP ARCH 300-320. 4th edition, Cisco Press, 2017.
8. Rak J., Papadimitriou D., Niedermayer H., Romero P. Information-driven network resilience: Research challenges and perspectives. Optical Switching and Networking, vol. 23, part 2, January 2017, pp. 156-178.
9. Lemeshko O., Yevdokymenko M., Yeremenko O., Mersni A., Segeč P., Papán J., Quality of Service Protection Scheme under Fast ReRoute and Traffic Policing Based on Tensor Model of Multiservice Network, 2019 International Conference on Information and Digital Technologies (IDT), 2019, pp. 288-295, doi: 10.1109/DT.2019.8813675.
10. Mersni, A., Ilyashenko, Vavenko T., Complex optimality criterion for load balancing with multipath routing in telecommunications networks of nonuniform topology, 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017, pp. 100-104, doi: 10.1109/CADSM.2017.7916095.

11. Lemeshko O., Yeremenko O. Linear optimization model of MPLS Traffic Engineering Fast ReRoute for link, node, and bandwidth protection, in Proc. 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 20-24 February 2018, pp. 1009-1013.
12. Lemeshko O., Garkusha S.V., Yeremenko O.S., Hailan A.M., Policy-based QoS Management Model for Multiservice Networks, in Proc. 2015 International Siberian Conference on Control and Communications (SIBCON), 21-23 May 2015, pp. 1-4.
13. Lemeshko A.V., Evseeva O.Yu., Garkusha S.V. Research on Tensor Model of Multipath Routing in Telecommunication Network with Support of Service Quality by Greate Number of Indices. Telecommunications and Radio Engineering, Vol. 73, Iss. 15, 2014, pp. 1339-1360.