Information & Security

Y. Ivanov
vol. 50, no. 2 (2021): 205-210
https://doi.org/10.11610/isij.5017

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Concepts in Networks and Communication Security and Graph Theory

Yordan Shterev Ivanov

National Military University "Vasil Levski," Veliko Tarnovo, Bulgaria
https://www.nvu.bg/

ABSTRACT:

In this article, the author presents concepts for exploring networks and communication security and recommendations for their use in the definition of requirements, reducing the risk of cyberattacks, and make some quantitative assessments. The focus is on the applications of graph theory in the analysis of communications and information networks.

ARTICLE INFO:

RECEIVED: 21 JUNE 2021
REVISED: 11 SEP 2021
ONLINE: 18 SEP 2021

KEYWORDS:

computer networks, communication technology, cybersecurity, graph theory

Introduction

The development of information technologies in hardware and software, on the one hand, and communications technologies on the other, have led to the possibility of accumulating large amounts of data and information and their rapid dissemination. There is a tendency to use increasingly complex and intelligent hacker attacks, which require the protection of hardware and software, individual devices, as well as information and communications networks. The purpose of this article is to analyze the concept of security of network communication and its characteristics and to present some basic concepts of graph theory, finding applications in the analysis of communications and information networks.

Network Security Concept

The protection (security) of an information and communication system (ICS) re-

E-mail: jshterev@abv.bg

quires finding a balance. The systems have their limitations. Finding a balance between safety and usability determines the usability of the system (see Fig.1). Finding the balance of an ICS in an organization is determined by the goals of the organization, the meaning of its protection, measuring the threats to protection. User-oriented systems have a high degree of usability and a low degree of safety. In contrast, internal systems may have a lower degree of usability but a higher degree of safety.

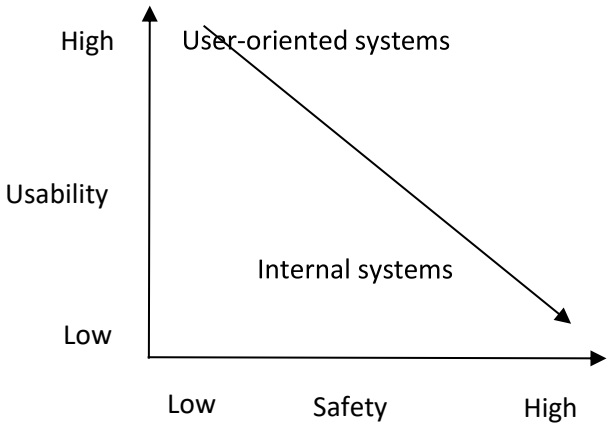

Figure 1: User-oriented systems and internal systems.

Goals of Protection

To achieve the protection, the following requirements have been adopted: [1,2]

- *confidentiality* – concerns the protection and confidentiality of information. Logical confidentiality involves storing and transmitting data, and physical confidentiality relates to hardware;
- *integrity* – ensures the accuracy of the information. The integrity of information is protected in two ways: storage and transmission. Users have confidence in the accuracy of the information, i.e., it is not modified when storing and transmitting it;
- *accessibility* – means that when a legitimate user needs the information, it is available. Archives, disk arrays, remote storage and other media are used to ensure accessibility.

Cyberattacks may violate the confidentiality, integrity or accessibility of information. The impact of cyberattacks and may include physical and financial damages, loss of reputation of the relevant institutions, and other negative effects.[3,4]

Assessing and Reducing Cyber Risk

Cyberattacks that exploit people are on the rise, as they are the weakest link in the security chain. The following recommendations could be made to reduce the risks of cyber attacks in communications.[5, 6, 7]

- Communicating cybersecurity risks is crucial;
- Understanding that people have limited processing capacity;
- The meaning of the information presented in the security risk messages must be clear;
- Providing clear and consistent guidelines for action, with security risk response options;
- Limiting the use of technical and security-specific terms and jargon;
- Carefully providing information on digital risk security, visual and verbal;
- Providing security assistance, advice, and documentation.

The analysis of risks related to communications and information security is a complex process. This is due to the complex connections in the communication networks and their practical realizations. Interruptions in connections between communicating nodes can lead to cascading failures. On the one hand, the consequences of attacks on a system of systems cannot be analysed only by assessing the behaviour of individual systems. It is necessary to assess the effect of systems' interdependencies on the behavior of the whole system of interest. Guariniello and DeLaurentis presented a method[8] that can be applied to analyse various cyberattacks, external and internal, as well as their effects on the communication links between nodes such as a ground station, two satellites, an aircraft (airplane, drone, helicopter), and a carrier.

Quantitative assessment of the risk of a cyber attack assigns a monetary value to the result. It is determined by:

- the expected loss of an asset – *LAE*:
- the exposure factor – a subjective potential part of the loss in a specific asset, if a specific threat has arisen.

$$LAE = asset\ value \times exposure\ factor$$

- estimate of the annual rate of occurrence (*ARO*), which determines the probability of the number of occurrence of an adverse event within a year.

At the end, the annual expectation of losses (*AEL*) is defined by:

$$AEL = LAE \times ARO.$$

Communication and information network nodes and information flows between them are often presented and explored using graph theory. It allows to derive some significant concepts.

Adjacency Matrix

For every graph, as well as the graphs of a multimedia presentation, such as for the graphs of a communication and information network, a matrix (**n x n**) of adjacency $A(G) = (a_{ij})$ of graph **G** has been defined as follows:

$$a_{ij} = \begin{matrix} 1, \text{if} v_i v_j \in E(G) \\ 0, \text{if} v_i v_j \notin E(G) \end{matrix}$$

V(G) is the set of graph's vertices, **E(G)** is the set of graph's edges. $\mathbf{v_i}, \mathbf{v_j} \in \mathbf{V(G)}$ and $\mathbf{v_i}\ \mathbf{v_j}$ is the edge connecting $\mathbf{v_i}$ and $\mathbf{v_j}$ vertices and $\mathbf{v_i v_j} \in \mathbf{E(G)}$. **n** is the number of vertices of the graph.

Consider a local network with *n* operating points and a network device (switch). Let the first row of the neighbourhood matrix represent the network drive, and all the other rows are computers, laptops, and others. Then the first row of the matrix has zero as the first element, and all other elements are ones. The remaining rows of the neighborhood matrix contain 1 for the first element (the edges indicating the connection to the network device), and all other elements are zeros.

Incidence Matrix

Besides, incidence matrix $B(G) = (b_{ij})$ [1] with dimension **(nxm)** has been defined for the graphs, determined from:

$$b_{ij} = \begin{cases} 1, \text{ if } v_i \text{ is the begining of the edge e}_j \\ -1, \text{ if } v_i \text{ is the end of the edge e}_j \\ 0, \text{ if } v_i \text{ and } v_j \text{ are not connected} \end{cases}$$

n indicates the number of the vertices in the graph, the number of the multimedia components of the media being used, respectively; **m** indicates the number of the edges of the graph.

If a local network with *n* operating points and a network device with an incidence matrix are expressed, then the edges are numbered sequentially from switch to workstations. The number of edges is equal to the number of operating points, which is the number of columns. Since the information passes in both directions, from the switch to the workstations and vice versa, the elements of the matrix different than zero, when exchanging information, take consecutive values "1" and "-1".

Reachability Matrix

It defines the reachability of information from one node to another node (object). Here it is possible to have subordination, priority between nodes. Reachability matrix is set by R(G) = (r_{ij}) with dimension (nxm). It is determined as follows:

$r_{ij} = 1$, if the v_j node is reachable from v_i

and

$r_{ij} = 0$, if the v_j node is not reachable from v_i.

A minimum base set of nodes may also be required so that the information is accessible to all other nodes.

Stavroulakis and Stamp, and Kavun et al. present methods for Internet analysis on the study of the interests.[9, 10] It is challenging to find mathematically defined methods for determining the significance of the activities or research of any author or scientist, which is why it is used in graph theory. The same method can be applied in any activity, regardless of its properties and characteristics.

Another work by Tamura and co-authors presents advances in applying graph theory to problems in communications, particularly in wireless networks.[11]

Through graph and network theory, relational network data are presented, suitable for registration deviations in the behavior of computer networks.[12] The detection of anomalies in computer networks, corporate, institutional, and others, requires fast computational capabilities, often parallel. The implementation of cyberattacks leads to a deviation from the normal behaviour of networks. Statistical models, Bayesian models, Markov chains, Monte Carlo series, and others are used to detect local anomalies.

Conclusions

The article indicates the basic requirements for the protection of information and communication networks. The concept of security of network communication and its characteristics are analyzed: network communication security concept, their requirements, recommendations to reduce the risk of cyberattacks, and quantitative assessment. In addition, some significant concepts related to the application of graph theory to communication and information networks are included. But this paper covered only some aspects of networking communication security.

More in-depth research on the application of graph theory as well as network theory on specific network structures is a future continuation of this article. Here, it is necessary to include specific cyber security policies with their associated requirements for software and hardware support.

Acknowledgements

This material is based upon work supported, in whole or in part, by the Department of Communication and Information System in the General Staff Faculty of "Vasil Levski" National Military University, Veliko Tarnovo.

References

1 Omar Santos and Michel Gregg, *Certified Ethical Hacker, Version 10,* Pearson Education (Sofia: Alex-Soft, 2020), Bulgarian edition.

2 Kamen Kalchev, *Measuring the Parameters of Cybersecurity Systems* (Sofia: "G.S. Rakovski" National Defence College, 2018). – in Bulgarian.

[3] Marcia W. DiStaso, "Communication Challenges in Cybersecurity," *Journal of Communication Technology* 1, no. 1 (2018): 43-60, https://joctec.org/archives/volume-1-issue-1/.

[4] Todor Tagarev, Salvatore Marco Pappalardo, and Nikolai Stoianov, "A Logical Model for Multi-Sector Cyber Risk Management," *Information & Security: An International Journal* 47, no. 1 (2020): 13-26, https://doi.org/10.11610/isij.4701.

[5] Jason R.C. Nurse, "Effective Communication of Cyber Security Risks," *7th International Scientific Conference on Security and Protection of Information (SPI 2013),* University of Oxford, 2013.

[6] Andrey Proletarskiy, Nikolay Rudenkov, Elena Smirnova, and Aleksandr Suvorov, Information Protection Technologies in Computer Networks (Moscow: Bauman State Technical University, 2021), - in Russian, https://intuit.ru/studies/courses/16655/1300/info.

[7] Erik Mayvold, Network Security, Self-learning course, in Russian, https://intuit.ru/studies/courses/102/102/info.

[8] Cesare Guariniello and Daniel DeLaurentis, "Communications, information, and cyber security in Systems-of-Systems: Assessing the impact of attacks through interdependency analysis," *Procedia Computer Science* 28 (2014): 720-727, https://doi.org/10.1016/j.procs.2014.03.086.

[9] Peter Stavroulakis and Mark Stamp, *Handbook of Information and Communication Security* (Berlin Heidelberg: Springer-Verlag, 2010).

[10] Sergii Kavun, Irina Mykhalchuk, Nataliya Kalashnykova, and Oleksandr Zyma, "A Method of Internet-Analysis by the Tools of Graph Theory," in *Proceedings of the 4th International Conference on Intelligent Decision Technologies (IDT´2012)*, *Gifu, Japan,* May 23-25, 2012, DOI: 10.1007/978-3-642-29977-3_4.

[11] Hiroshi Tamura, Keisuke Nakano, Masakazu Sengoku, and Shoji Shinoda, "On applications of graph/network theory to problems in communication systems," *ECTI Transactions on Computer and Information Technology* 5, no. 1 (May 2011), 8-14, https://doi.org/10.37936/ecti-cit.201151.54227.

[12] Niall Adams and Nicholas Heard, *Data Analysis for Network Cyber-Security* (Heilbronn Institute for Mathematical Research, University of Bristol Imperial College Press, 2014).

About the Author

Yordan **Shterev** received the M.S. degree from Sofia University "St. Kliment Ohridski," Faculty of Physics, in 1983, and a Ph.D. degree from the "G.S. Rakovski" Natinonal Defence College in 2007. Currently, he is an Associate Professor in the "Communications and Information Technology" Department of the National Military University "Vasil Levski," Veliko Tarnovo. His research interests are in data mining, time synchronization of multimedia, and Cybersecurity. He is a senior member of the Union of Bulgarian Scientists and the Union of Automatics and Informatics. https://orcid.org/0000-0001-7874-6935