Opinion

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology
ISSN 2349-3917

2022
Vol.10 No.9:001

Use of Information and Communication Technologies for Collecting Information in Embedded Computer Networks

Igor Kotenko*

Departmet of Computer and Space Engineering, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia

***Corresponding author:** Igor Kotenko, Departmet of Computer and Space Engineering, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia Email : Igorkoten985@gmail.com

Received date: August 02, 2022, Manuscript No. IPACSIT-22-15002; **Editor assigned date:** August 04, 2022, PreQC No. IPACSIT-22-15002 (PQ); **Reviewed date:** August 12, 2022, QC No IPACSIT-22-15002; **Revised date:** August 22, 2022, Manuscript No. IPACSIT-22-15002 (R); **Published date:** September 01, 2022, DOI: 10.36648/ 2349-3917.10.9.1

Citation: Kotenko I (2022) Use of Information and Communication Technologies for Collecting Information in Embedded Computer Networks. Am J Compt Sci Inform Technol Vol. 10 Iss No.9:001.

Description

Embedded computer networks are gaining popularity nowadays. Examples of their implementation are IoT networks, robotic networks, sensor networks, etc. Embedded computer networks should be considered as highly developed systems with a multilevel hierarchical structure. To manage such complex, branched and nonlinear systems, it is necessary to search for and use innovative approaches to predict the development of events in order to develop correct and operational control decisions. The use of information and communication technologies for collecting information in embedded computer networks enables an attacker to influence these networks by implementing cyber-attacks. The impact of cyber-attacks is possible due to the massive use of outdated operating systems, ineffective protection mechanisms and the presence of multiple vulnerabilities in unprotected network protocols. The exploitation of such vulnerabilities gives a potential attacker the ability to change the settings of built-in network devices, listen and redirect traffic, block network communication, and gain unauthorized access to the internal components of embedded computer networks. In this case, cyber-attacks should be considered as one of the key factors that determine the survivability of embedded computer networks. In this case, survivability is understood as the ability of an embedded computer network to retain the properties necessary to fulfill a given purpose in conditions of complex use by an attacker of countermeasures not provided for by the conditions of normal operation.

Detection and Analysis of Anomalous Network Traffic Activity

The survivability of an embedded computer network is estimated by the downtime ratio, which is characterized by the probability that the network will be in an inoperative state at an arbitrary moment in time. Since the impact of cyber-attacks in most cases leads to disruption of the network performance and disruption of information exchange in it, the likelihood of successful implementation of cyber-attacks has the same physical meaning as the downtime rate. Despite the existence of many solutions for protecting computer networks from cyber-attacks for example, Arbor Networks, this research topic is still relevant. Of particular importance are the methods and approaches associated with the detection and analysis of anomalous network traffic activity caused by the impact of cyber-attacks. This direction makes it possible to implement early detection of cyber-attacks. All this gave rise to the search for new methods of detecting and predicting cyber-attacks. The impact of cyber-attacks leads to the appearance of anomalous activity in the traffic of embedded computer networks. There are many factors to consider in order to continuously monitor and detect abnormal network traffic activity. These factors include: (1) the presence of a large number of network routes on which periodically sharp fluctuations in data transmission delay and large packet losses occur, (2) the emergence of new properties of network traffic, (3) the need to ensure high quality of application service, etc.

Method for Ensuring the Survivability of an Embedded Computer Network in Conditions of Cyber-Attacks

The aim of the paper is to suggest a method for ensuring the survivability of an embedded computer network in conditions of cyber-attacks, based on identifying anomalies in network traffic by assessing its self-similarity and determining the type of impact of cyber-attacks using statistical methods. The idea of applying the theory of fractals to the analysis of network traffic has been confirmed in many studies. It is based on the fact that the self-similarity index can serve as some integral label that determines many properties of traffic, including the type of information transmitted over the network and the presence or absence of anomalies. Statistical methods and approaches, despite their already existing rather deep study, continue to attract interest in works related to the detection of computer attacks, as they are based on a sufficiently substantiated and correct mathematical foundation. Therefore, the approach proposed in this paper, based on the integration of methods of fractal and statistical analysis, in our opinion, should lead to an increase in the efficiency of detecting computer attacks. The

novelty of the paper lies in the fact that it substantiates an effective method for detecting anomalies in network traffic based on the analysis of its self-similarity. These anomalies can correspond to the early stages of various cyber-attacks. Statistical methods make it possible to increase the accuracy of determining the self-similarity indicator of traffic in conditions of non-stationary traffic, which is a significant difference and advantage of the proposed method. The paper proposed a new method for detection of cyber-attacks, combining the principles of fractal analysis of network traffic and mathematical statistics, which ensure the survivability of an embedded computer network. The main methods for assessing self-similarity are the Dickey-Fuller test, R/S analysis and the DFA method. As methods of mathematical statistics, the methods of moving average, streaming windows and cumulative sums are used.