UDC 004.93
DOI: 10.31891/CSIT-2021-5-4

SERGII LYSENKO, DMYTRO SOKALSKYI, IANA MYKHASKO
Khmelnytskyi National University, Khmelnytskyi, Ukraine

METHODS FOR CYBERATTACKS DETECTION IN THE COMPUTER NETWORKS AS A MEAN OF RESILIENT IT-INFRASTRUCTURE CONSTRUCTION: STATE-OF-ART

The paper presents a state-of-art of the methods for cyberattacks detection in the computer networks. The main accent was made on the concept of the resilience for the IT infrastructure. The concept of cyber resilience in the terms of cybersecurity was presented. The survey includes the set of approaches devoted to the problem of construction resilient infrastructures. All investigated approaches are aimed to construct and maintain infrastructure's resilience for cyberattacks resistance. Mentioned techniques and frameworks keep the main principles to assure resilience. To do this there exists some requirements to construct such infrastructure: IT infrastructure has to include the set ready to use measures of preparation concerning the possible cyber threats; it must include the set of special measures for the protection, as well as for cyberattacks detection; important issue and required is the possibility to respond the attack and to be able to absorb the negative attacks' impact; IT infrastructure must be as adaptive as it is possible, because today the dynamic of the attacks mutation is very high; IT infrastructure must be recoverable after the attacks were performed. In addition, the state-of-art found out that known approaches have domain-specific usage and it is important to develop new approaches and frameworks for the cyberattacks detection in the computer networks as a means of resilient IT-infrastructure construction.

Keywords: cyberattack, IT infrastructure, malware, computer systems, resilience, detection efficiency, network traffic

СЕРГІЙ ЛИСЕНКО, ДМИТРО СОКАЛЬСЬКИЙ, ЯНА МИХАСЬКО
Хмельницький національний університет

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ КІБЕРАТАК В КОМП'ЮТЕРНИХ МЕРЕЖАХ ЯК ЗАСОБІВ ДО ПОБУДОВИ РЕЗИЛЬЄНТНИХ ДО ВТОРГНЕНЬ ІТ-ІНФРАСТРУКТУР

ІТ-інфраструктура стає все більш взаємопов'язаною, тоді як кіберзагрози для критичної інфраструктури стають все більш складними, від яких важко захиститися. Кібербезпека акцентує увагу на створенні засобів захисту, щоб запобігти втраті конфіденційності, цілісності та доступності цифрової інформації та систем, але останніми роками кібератаки продемонстрували, що жодна система не є непроникною. Кібер резильєнтність стала додатковим пріоритетом, який спрямований на те, щоб ІТ-інфраструктури могли підтримувати суттєві рівні продуктивності, навіть якщо можливості погіршуються внаслідок кібератаки. У статті представлено сучасні методи виявлення кібератак у комп'ютерних мережах. Основний акцент був зроблений на концепції стійкості для ІТ-інфраструктури. Було представлено поняття кіберстійкості з точки зору кібербезпеки. Дослідження включає комплекс підходів, присвячених проблемі побудови резильєнтних інфраструктур. Усі досліджувані підходи спрямовані на створення та підтримку резильєнтності інфраструктури до кібератак. Згадані методи та фреймворки зберігають основні принципи забезпечення резильєнтності. Для цього існують певні вимоги до побудови такої інфраструктури: ІТ-інфраструктура повинна включати набір готових до використання заходів підготовки щодо можливих кіберзагроз; має включати комплекс спеціальних заходів щодо захисту, а також виявлення кібератак; важливою і необхідною проблемою є можливість реагувати на атаку та мати можливість поглинати вплив негативних атак; ІТ-інфраструктура має бути максимально адаптивною, тому що сьогодні динаміка мутації атак дуже висока; ІТ-інфраструктура повинна бути відновлена після здійснення атак. Крім того, сучасний дослідження показало, що відомі підходи мають нішеве застосування і важливо розроблювати нові підходи та засоби для виявлення кібератак у комп'ютерних мережах як засобу побудови резильєнтних ІТ-інфраструктур.

Ключові слова: шкідливе програмне забезпечення, живучість, комп'ютерні системи, достовірність виявлення, кібератака, мережний трафік.

Introduction

IT infrastructures have deeply into all aspects of our life. The cyber-physical systems based on the different infrastructures are a new concept today and are the next generation of system that must secure and be ready to resist the cyberthreats today [1-9]. In recent years, network cyberattacks on the IT infrastructure of information systems is still growing [10-14]. Thus, in June 2010, the security experts have found a botnet attack “StuxNet”, which threated the industrial system, infected with computer systems and networks around the world [15].

Since the botnet malware StuxNet have appeared, a great variety of new cyber threads IT infrastructure had appeared [16-17]. Furthermore, new attacks involve new approaches and system information, that makes it possible to overcome the protection of IT infrastructure. That's why there exists an important task to investigate, maintain, and develop new methods for cyberattacks detection in the computer networks as a mean of resilient IT-infrastructure construction.

This research is a state-of-art of the methods for cyberattacks detection in the computer networks, that present the set of approach devoted to the problem of construction of resilient IT-infrastructures.

Concept of cyber resilience

Nowadays, the problem of cyber defense is not only issue of protection of infrastructure. The very new concept is the resilience [14].The concept of resilience is applied to a lot of contexts as well as to IT infrastructures. For instance, in the ecology the resilient item is a kind of population property that is able to survive. This concept is used in economics, construction industry [15] etc.

In the term of cybersecurity and it usage for IT infrastructure, the concept of resilience is the special ability to execute the resistance, restoration and adaption in the situation of cyberattacks performing [18-20].

So, the importunate of the development of IT infrastructure resilience is very significant.

Techniques for resilient IT infrastructures construction

Today there is a huge number of approaches devoted to cybersecurity. But task of cyber resilience is not solved yet. Nevertheless, researches make attempts to bring new techniques to construct the IT infrastructures more resilient against the cyber threads.

In [21] the technique for resilient cyber-physical systems construction is proposed. It is devoted to the task of detection of the communication delays in the infrastructure networks in the situation of denial-of-service (DoS) attacks.

The approach previously was based on the usage of multiagent systems (MASs) in order to identify the DoS attacks. The next-gen approach is based on the distributed resilient technique, that involves as the mathematical tools technique a general heterogeneous linear multiagent systems. It enables the possibility to deal with the nonuniform communication delays.

The core of the approach is the usage of the kinds of observers, that are sampled-based. To make the approach more efficient the authors proposed to make the observers be adaptive and distributed. This idea was achieved by using a buffer mechanism, that made it possible to eliminate the heterogeneous behavior generated by communication delays. In the terms of the adopting of the adaptive distributed resilient observers, the techniques made it possible to develop the resilient mechanism able to resist the denial-of-service attacks. In addition, authors included a time-varying sampling period sequence in order to prevent the attack implementation and its detection by the sampling period of the possibly infected infrastructure.

For the purpose to verify the overall technique efficiency, using the provided resilient observers, a special system controller for detection was developed. Its implementation and the series experiments conducting has proved the effectiveness of the prosed technique for resilient cyber-physical systems.

An approach for resilient control of cyber-physical systems was proposed in [22]. It is a technique for the resilient Cyber-Physical Systems construction.

In the research the authors tried to simulate different situations that may cause with IT infrastructures during its functioning. The core of the idea is to develop the system that must support the correct operations set for the crucial functional elements notwithstanding providing the resistant misbehavior.

The technique uses a moving target defense paradigm. The main idea is to deal with the linear switching of state-space matrices. The approach involves both the physical and network layers concerning a control system presented in network.

The efficiency of the proposed technique was substantiated by the set of experiments. The results have showed that appliance of the technique for the systems had made it possible to maintain systems' stability. We also evaluate, via simulation, a step-by-step procedure that takes a transfer function, representing the dynamics of the physical process.

In addition, author proved that the involvement of the approach made it possible to develop the resilient IT infrastructure, where there is a topology of decentralized controllers.

In [23] an approach for the constructing of the resilient systems against the cyberattack is proposed. Authors presented that today there is a strong need to protect the infrastructures under the attacks. To do this the cybersecurity issue must be organized around the main terms of confidentiality, integrity and availability. In addition, the main problem and drawbacks of cybersecurity of the IT- infrastructures is its strong increasing. In this situation, the cybersecurity for the IT- infrastructures has become unable to take into account the huge aspects as the time dynamics of time, space bound behavior, rapid changes etc.

In the approach the authors proposed the analysis of construction aspects concerning the resilient systems under the cyberattack.

The main idea is that there is a need to make the cyberattack resilient missions, that will give the opportunities to achieve the completion of resilient mission goals. Also, it will give the possibility to provide the IT assets and the needed services, which will enable the support of the resilient actions concerning the attacked system.

The research presents also a set of architectural issues in order to construct proper cyberattack resilience missions. It involves the mission-centricity, survivability (using the adaptation procedure). In addition, it includes the mission C2, cybersecurity management mission to achieve the efficient mission execution.

To perform the evaluation of the effectiveness of the proposed approach, the authors have developed the resilient IT infrastructure, that includes two multi-agent systems. These systems are adaptive and have possibility to interact. Furthermore, researchers presented a set of models and algorithms, defined for the proposed resilient system with the experimental results.

In [24] an approach for the resilient cyber-physical systems construction is presented. It includes the set of steps for the development of an updated state estimation process, that is aimed to increase the resilience of IT-infrastructures under the cyberattacks.

Authors of the technique proposed to involve the existing data, that are presented in the current state estimators. The main idea of the approach is to establishes the state estimation vulnerability concerning the cyberattacks that are able to execute the data injection target at evading detecting by the mean of the outlier routines, that are used in the situation of the estimation processes.

In addition, the researchers presented the set of architectural solutions based on usage of the emerging smart grid technologies.

In [25] an agent-based cyber control strategy design for resilient control systems was produced. It presents an approach directed into defense of the critical infrastructure.

Mentioned approach includes several sets:

1) development of the cyber security research built into the industrial control system environment. The system involves the set of mechanisms to present opened and closed loop, feedback, designs.

2) integration of the cyber-physical design. It has to ensure the possibility to utilize the system data for correct response on the physical system.

3) integration of the techniques that are able to address a new approach to distributed IT infrastructures. , which considers both the industrial process control dynamics for SES, as well as the influences of the benign and malicious human.

In [26] a technique for resilient cyber-physical systems construction was presented.

In the research the authors proposed several contributions to ensure cybersecurity and infrastructure resilience. To do this the framework WAMPAC was developed. It is the security frame work, tht makes it possible to provide the end-to-end attack-resilient IT infrastructure in the power grid.

The approach involves the cybersecurity issues:

1) framework maintains the infrastructure life cycle (such as risk assessment, cyberattacks prevention measures, cyberattacks detection procedures, cyberattacks mitigation measures);

2) framework involves a defense-in-depth principles that combines the combines the cyberattacks resilience at IT infrastructure and the software levels;

3) framework is able to detect the cyber–physical security anomalies.

The authors also have presented a set of cyberattack-resilient algorithms, such as anomaly detection and mitigation approaches. The paper includes the set of experiments that prove the efficiency of the frame work. To do this it presents some cases how to prevent, detect and mitigate the attacks.

In [27] research devoted to the theoretical and some practical issues concerning the resilience of IT infrastructures are presented.

The paper shows the vast importance of the resilience today, as it can increase the adversary’s effort level for the needed for the malicious objectives achievement. In terms of resilient infrastructure, it must be highly resistant to malware activities and can be able to prevent the cyberattacks execution.

The author proposed to construct systems, that were able to evaluate resilience in the presence of cyberattacks. The research involves the game-based simulation framework, that demonstrates the process of attack as well as the defending procedure.

An approach also shows a set of simulations of sufficient fidelity. To do this the manuscript includes the description of complex heterogeneous simulations. The framework is modeling integration tool names SURE for infrastructure against the cyberattacks.

The inbuild modeling simulator uses the models, constructed with the use of a model-based integration tool the heterogeneous and distributed simulations. It is able to perform the construction of the rapid design, synthesis, and evaluation of experiments.

The main feature of the SURE framework is the possibility to make the transportation systems. In this case the framework is able to provide the needed domain-specific languages, specified models, tools for the translation of constructed models. The proposed framework has in-built simulation driver tool. It’s main aim is to perform the establishment of a coherent experimentation environment.

Conclusions

The paper presents a state-of-art of the methods for cyberattacks detection in the computer networks. The main accent was made on the concept of the resilience for the IT infrastructure. The concept of cyber resilience in the terms of cybersecurity was presented. The survey includes the set of approaches devoted to the problem of construction resilient infrastructures. All investigated approaches are aimed to construct and maintain infrastructure’s resilience for cyberattacks resistance. Mentioned techniques and frameworks keep the main principles to assure resilience. To do this there exists some requirements to construct such infrastructure:

1) IT infrastructure has to include the set ready to use measures of preparation concerning the possible cyber threats;

2) it must include the set of special measures for the protection, as well as for the cyberattacks detection;

3) important issue and required is the possibility to respond the attack and to be able to absorb the negative attacks' impact;

4) IT infrastructure must be as adaptive as it is possible, because today the dynamic of the attacks mutation is very high;

5) IT infrastructure must be recoverable after the attacks were performed.

In addition, the state-of-art found out that known approaches have domain-specific usage and it is important to develop new approaches and frameworks for the cyberattacks detection in the computer networks as a means of resilient IT-infrastructure construction.

References

1. McAfee Mobile Threat Report Q2, 2021. URL: https://www.mcafee.com/content/dam/cons umer/en-us/docs/2020-Mobile-Threat-Report.pdf. (accessed 10.10.2021).

2. S. Liu, B. Xu, S. Li and Y. Liu, Resilient control strategy of cyber-physical system under DoS attacks, *36th Chinese Control Conference (CCC)*, 2017, pp. 7760-7765, doi: 10.23919/ChiCC.2017.8028584.

3. X. Koutsoukos et al., SURE: A Modeling and Simulation Integration Platform for Evaluation of Secure and Resilient Cyber–Physical Systems, *Proceedings of the IEEE*, vol. 106, no. 1, pp. 93-112, Jan. 2018, doi: 10.1109/JPROC.2017.2731741.

4. A. M. Melin, E. M. Ferragut, J. A. Laska, D. L. Fugate and R. Kisner, A mathematical framework for the analysis of cyber-resilient control systems, *6th International Symposium on Resilient Control Systems (ISRCS)*, 2013, pp. 13-18, doi: 10.1109/ISRCS.2013.6623743.

5. L. Zhang, X. Chen, F. Kong and A. A. Cardenas, Real-Time Attack-Recovery for Cyber-Physical Systems Using Linear Approximations, *IEEE Real-Time Systems Symposium (RTSS)*, 2020, pp. 205-217, doi: 10.1109/RTSS49844.2020.00028.

6. A. Lukina, A. Tiwari, S. A. Smolka, L. Esterle, J. Yang and R. Grosu, Resilient Control and Safety for Cyber-Physical Systems, *IEEE Workshop on Monitoring and Testing of Cyber-Physical Systems (MT-IT INFRASTRUCTURES)*, 2018, pp. 16-17, doi: 10.1109/MT-IT INFRASTRUCTURES.2018.00015.

7. C. Deng and C. Wen, MAS-Based Distributed Resilient Control for a Class of Cyber-Physical Systems With Communication Delays Under DoS Attacks, *IEEE Transactions on Cybernetics*, vol. 51, no. 5, pp. 2347-2358, May 2021, doi: 10.1109/TCYB.2020.2972686.

8. S. Sulochana and V. Manjula, Resilient system for secure sharing of information against false data injection attack, *International Conference on Information Communication and Embedded Systems* (ICICES), 2016, pp. 1-5, doi: 10.1109/ICICES.2016.7518943.

9. Lysenko, S., Bobrovnikova, K., Savenko, O., Shchuka, R. Technique for Cyberattacks Detection Based on DNS Traffic Analysis, *CEUR-WS*, Vol 2732. ISSN: 1613–0073. 2020. pp. 171-182

10. Bobrovnikova, Kira, Sergii Lysenko, Piotr Gaj, Dmytro Denysiuk "Technique for IoT Cyberattacks Detection Based on DNS Traffic Analysis.CEUR-WS.Vol.2623. ISSN: 1613–00732020, pp. 208-218.

11. Sergii Lysenko, Kira Bobrovnikova, Peter Popov, Viacheslav Kharchenko, Dmytro Medzatyi. Spyware Detection Technique Based on Reinforcement Learning. *CEUR-WS.*Vol. 2623 ISSN: 1613–0073 (2020), pp. 307-316

12. Lysenko, S., Bobrovnikova, K., Matiukh, S., Hurman, I., Savenko, O.Detection of the botnets' low-rate DDoS attacks based on self-similarity. *International Journal of Electrical and Computer Engineering*, ISSN 2088-8708, 2020, 10(4), pp. 3651-3659.

13. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., Vasylkiv, N. Botnet detection approach based on the distributed systems. *International Journal of Computing*, ISSN 1727-6209, 2020, 19(2), pp. 190-198.

14. Sergii Lysenko, Kira Bobrovnikova, Peter Popov, Viacheslav Kharchenko, Dmytro Medzatyi. Spyware Detection Technique Based on Reinforcement Learning. CEUR-WS.Vol. 2623 ISSN: 1613–0073 (2020), pp. 307-316

15. S. Al-Rabiaah, The "Stuxnet" Virus of 2010 As an Example of A "APT" and Its "Recent" Variances, *21st Saudi Computer Society National Computer Conference (NCC)*, 2018, pp. 1-5, doi: 10.1109/NCG.2018.8593143.

16. Lysenko S.., Bobrovnikova Y., Kharchenko V. Methods of detecting botnets in computer systems. *Modern information systems.* 2019. Т.3. №4. С.87-95.

17. Sergii Lysenko, Kira Bobrovnikova, Piotr Gaj, Tomas Sochor, and Iryna Forkun Resilient Computer Systems Development for Cyberattacks Resistance. *CEUR-WS*. 2021, 2853, pp. 353–361.

18. Cimellaro G. P., Dueñas-Osorio L., Reinhorn A.M. Introduction to special issue on resilience-based analysis and design of structures and infrastructure systems. Structural Engineering, 2016, No. 142(8), pp.1-5.

19. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A. Resilience metrics for cyber systems. Environment Systems and Decisions, 2013, No. 33(4), pp. 471-476.

20. Bodeau, D.J., Graubart, R. D. Cyber resiliency design principles: selective use throughout the lifecycle and in conjunction with related disciplines. MITRE Corp., Tech. Rep., 2017, p.98.

21. C. Deng, Distributed Resilient Control for Cyber-Physical Systems under Denial-of-Service Attacks, *23rd International Conference on Mechatronics Technology (ICMT)*, 2019, pp. 1-5, doi: 10.1109/ICMECT.2019.8932108.

22. M. Segovia-Ferreira, J. Rubio-Hernan, R. Cavalli and J. Garcia-Alfaro, Switched-Based Resilient Control of Cyber-Physical Systems, *IEEE Access*, vol. 8, pp. 212194-212208, 2020, doi: 10.1109/ACCESS.2020.3039879.

23. G. Jakobson, Mission-centricity in cyber security: Architecting cyberattack resilient missions, *5th International Conference on Cyber Conflict* (CYCON 2013), 2013, pp. 1-18.

24. S. Hopkins, E. Kalaimannan and C. S. John, Foundations for Research in Cyber-Physical System Cyber Resilience using State Estimation, *SoutheastCon*, 2020, pp. 1-2, doi: 10.1109/SoutheastCon44009.2020.9249745.

25. C. Rieger, Q. Zhu and T. Başar, Agent-based cyber control strategy design for resilient control systems: Concepts, architecture and methodologies, *2012 5th International Symposium on Resilient Control Systems*, 2012, pp. 40-47, doi: 10.1109/ISRCS.2012.6309291.

26. A. Ashok, M. Govindarasu and J. Wang, Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid, *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389-1407, July 2017, doi: 10.1109/JPROC.2017.2686394.

27. X. Koutsoukos et al., SURE: A Modeling and Simulation Integration Platform for Evaluation of Secure and Resilient Cyber–Physical Systems, *Proceedings of the IEEE*, vol. 106, no. 1, pp. 93-112, Jan. 2018, doi: 10.1109/JPROC.2017.2731741.

Sergii Lysenko **Сергій Лисенко**	Doctor of Science, Professor of Computer Engineering & System Programming Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: sirogyk@ukr.net. orcid.org/0000-0001-7243-8747, Scopus Author ID: 54420643500, ResearcherID: I-1728-2018 https://scholar.google.com.ua/citations?hl=uk&user=TuAfytwAAAAJ&view_op=list_works	доктор технічних наук, професор кафедри комп’ютерної інженерії та системного програмування, Хмельницький національний університет, Хмельницький, Україна
Dmytro Sokalskyi **Дмитро Сокальський**	Master student, Computer Engineering, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: sokalskij7@gmail.com	студент, комп’ютерна інженерія, Хмельницький національний університет, Хельницький, Україна.
Iana Mykhasko **Яна Михасько**	Master student, Computer Engineering, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: yashamyy@gmail.com	студентка, комп’ютерна інженерія, Хмельницький національний університет, Хельницький, Україна.