

Graph-based evaluation of probability of disclosing the network structure by targeted attacks

Andrei Privalov¹, Ekaterina Skudneva¹, Igor Kotenko², and Igor Saenko²

¹Emperor Alexander I St. Petersburg State Transport University (PGUPS), Saint-Petersburg, Russia

²St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Saint-Petersburg, Russia
apivalov@inbox.ru, evskudneva@gmail.com, {ivkote, ibsaen}@comsec.spb.ru

Abstract— Protecting data transmission networks from targeted attacks is currently a priority cyber security goal in critical infrastructures. The paper considers the approach to the evaluation of the probability of disclosing the structure of the data transmission network when the attacker implements targeted attacks. The approach is based on graph theory. The conceptual model of the targeted attack is presented. Algorithms for estimating the structural secrecy of data transmission networks are developed. They include an algorithm for evaluating the probability of compromising a network node and recognizing the structure of the data transmission network, as well as a generalized algorithm for estimating the structural secrecy. Implementation and results of the experimental evaluation of the proposed approach are discussed.

Keywords— data transmission network, structural secrecy, targeted attack, attack detection

I. INTRODUCTION

Nowadays, computer security specialists pay a lot of attention to the development of approaches and methods of protection against targeted attacks. This is especially important for protection of data transmission networks in critical information infrastructures where technological processes are implemented. Examples of such networks are large-scaled railway, oil and gas transmission networks, power grids, etc. A distinctive feature of targeted attacks is their purposeful and unique character. The main purpose of these attacks is to disrupt the main control and technological processes. Targeted attacks are distinguished from other attacks by their high complexity, multi-dimensionality and long time length. Targeted attack objects are specific automated systems or telecommunication networks. As a rule, the initial stage of the targeted attack is to disclose the network structure. This is followed by the stages of studying network elements (network reconnaissance), fulfilling the harmful actions and destroying the attack presence traces.

Usually, technological control processes are mapped into data transmission networks. This mapping affects the number and time of correspondents, the amount of data transferred, the location of information sources, etc. Targeted attack can detect all this information by analyzing the traffic of the data transmission network and the space of IP-addresses used in it. As a result, data transmission networks have a number of unmasking features that can be detected by targeted attacks. Such features include, for example, topology, network type and structure, and network software configuration.

Collection and analysis of unmasking features during targeted attacks allow one to determine with high accuracy the purpose and location of computer or network devices in the technological processes. If the attacker knows the purpose of the device, he (she) can determine the importance of the information circulating in the data transmission network. Further, the attacker can recognize the nodes of the network and their interaction with the rest of the network. Thus, it can recognize the stage of the technological process being implemented. As a result, the attacker can cause quite a lot of damage both to the data transmission network and to the entire technological processes in the information infrastructure.

The specifics of the targeted attacks discussed above determine the great importance of combating the attacks of this type. The research in this scientific field mainly focuses on methods of detecting targeted attacks. However, none of the known methods of detecting the targeted attacks can guarantee that such attacks may remain undetected. Therefore, data transmission network developers should consider the possibility of implementing targeted attacks and assess the risks that arise. This determines the great importance of the problem of evaluating the probability of disclosing the network structure under implementation of targeted attacks and design the methods of its solution.

The main goal of the paper is to consider a new approach to evaluate the probability of disclosing the data transmission network structure, based on the analysis of graphs specifying this structure.

This approach is, on the one hand, easy enough to implement and, on the other hand, could be efficient. The main contribution of the paper is as follows:

- Development of a model of the targeted attack against the data transmission network.
- Development of graph-based algorithms for recognition of data transmission network structure and assessment of the network structural secrecy.
- Software implementation of the proposed approach, its experimental evaluation and analysis.

The paper has the following structure. The analysis of the related work is provided in Section II. In Section III the theoretical foundations are considered. The conceptual model of the targeted attack and the algorithms for evaluation of the probability of disclosing the data transmission network structure are presented in this section. Section IV is devoted to the implementation of the proposed approach. Section V represents the experimental results. Section VI contains the main conclusions and formulates the future research directions.

II. RELATED WORK

The topic of information security during the implementation of targeted attacks is very popular in the scientific community. For example, [1] proposes to focus on the development of a strategy for an in-depth system of protection against targeted attacks. The main task of this system should be to constantly monitor networks and security controls. [2] shows that targeted attacks are the result of the evolution of computer attacks, changing technologies of their implementation and behavioral changes of intruders.

[3] distinguishes the following classes of detection methods for multi-step cyberattacks (all targeted attacks are also multi-stepped): similarity-based, causal correlation, structural-based, case-based, and mixed ones. However, in this classification the graph-based methods (as part of structural-based ones) use attack graphs, not graphs of network structures.

Promising methods of detection and classification of targeted attacks are machine learning methods, such as Support Vectors Machine (SVM) [4], Opinion Dynamics [5], Perfect Bayesian Nash Equilibrium (PBNE) [6] and others. Anomaly detection methods in log events and their comparison with the rules already determined are suggested in [7]. For successful network intrusion detection, [8] proposes to detect and monitor the anomalies in the data transmission network. Based on the analysis of anomalies in the network, [9] offers different methods of evaluating the obtained data. At the same time, it is necessary to carry out real data network monitoring based on big data processing [10]. This causes a large amount of data to be considered. Such task involves identifying and calculating metrics from the data transmission network traffic.

[11] suggests rating suspicious hosts and focusing the analysis on a small sample of hosts. [12] proposes thread-based intrusion detection techniques. [13] offers to monitor the amount of data, time and size of packets when analyzing the network traffic. [14] shows that the addition of time interval analysis capabilities to this approach allows one to identify and classify existing and unknown botnets. [15] analyzes the possibilities of the signature intrusion detection methods and demonstrated the capability of various special network routing protocols to facilitate intrusion detection.

Graph theory is often applied to analyze computer security metrics. [16-19] propose an approach to analytical modeling of attacks based on the application of attack modeling principles for analyzing events occurring in real time, multi-level representation of attack graphs and service dependencies, and the use of known and expected vulnerabilities for constructing attack graphs.

In [20], the problems associated with the use of attack graphs and methods for resolving them are considered. These methods include handling inaccuracies in determining the pre- and post-conditions for performing attack actions, processing cycles when using Bayesian output to analyze the attack graph, and displaying incidents on the graph attacks, as well as automatic selection of protective measures in case of a high level of risk. A software prototype of the cybersecurity monitoring system and experimental results are presented.

[21] proposes the graph analytical metric to evaluate the mitigation of targeted attacks. To detect network vulnerabilities, [22] considers distances between graph nodes and use them in attack graph analysis. [23] suggests to generate

a set of user attributes and apply them to generate behavior profiles. If the attributes differ from the usual ones, then intrusion detection for the data network is possible.

Our paper also proposes to analyze the network traffic to identify anomalies in data transmission networks. For this purpose, in accordance with the technological process, graph sets are formed and compared with the observed data flow using the graph isomorphism algorithm [24]. As an isomorphism algorithm for large graphs, it is possible to use the algorithm proposed in [25] to scale the network. A common graph database that can be used to map graphs and check them for isomorphism validity is introduced in [26]. [27] demonstrates that when analyzing the traffic in data transmission networks using the proposed methods of applying the graph isomorphism algorithm, it is possible to detect significant patterns of information dissemination through a social network.

Thus, despite the fact that there are a number of works on the topic of protection against targeted attacks, which offer a variety of methods of their detection and classification, the task of evaluating the probability of disclosing the structure of the data transmission network when implementing targeted attacks remains unresolved. The proposed graph-based approach to this task allows one to identify bottlenecks in the network and identify targeted attacks at the initial stage of their implementation.

III. THEORETICAL FOUNDATIONS

A. Targeted attack model (for network structure disclosing)

According to some studies, today the average cost of just a single targeted attack on a large organization is more than US\$6 million [28]. This determines the importance of any method of defense against such attacks, including the method we offer. Targeted attacks use various implementation methods, but at the same time they all have common features that allow one to build a common targeted attack model.

Communication devices and user terminals are characterized by a set of unmasking features at all stages of the technological process. Each unmasking feature has its own specific information, allowing one to identify the control object with some probability.

All unmasking features related to the process are determined by the technical characteristics of the data transmission network elements and their software. The set of unmasking features associated with a data transmission network is determined by the structure of that network, interfaces, protocol stacks, and software.

The structure of the network can be classified according to the following characteristics:

- Directions of distribution of data flows.
- Parameters of switching networks.
- Characteristics of changes in route-address information.
- Characteristics of changes in information load.

At implementation of the first stage of a targeted attack, when the technological process is monitored, it is possible to establish unmasking features. Such features also include corresponding pairs in the IP-address space. The analysis of such pairs allows one to determine the following information:

- Location of telecommunication equipment.
- With what device and when does this equipment interact?
- Which stage of the process control cycle does information exchange take place for?
- What is the intensity of the information exchange?
- How does this relate to the process being implemented?

Having this information, the attacker can easily disclose the network structure, carry out a computer attack and damage the information infrastructure.

Thus, the monitoring of the data transmission network makes it possible to determine when the most responsible stage of management is realized and when the impact on the data network will cause, among other things, significant economic damage.

The central units of the targeted attack model are unmasking feature collection systems. These include the following subsystems (Fig. 1):

- Monitoring and analysis of the network topology (network scanner).
- Traffic control subsystem (network sniffer).
- Information source location determination subsystem.

Operation with the received data is performed in the decision making subsystem.

As a result, the network is disclosed, and a set of reference graphs reflecting different technological processes is formed. Thus, targeted attacks implement the principles of intelligence processing and analysis in the data transmission network space.

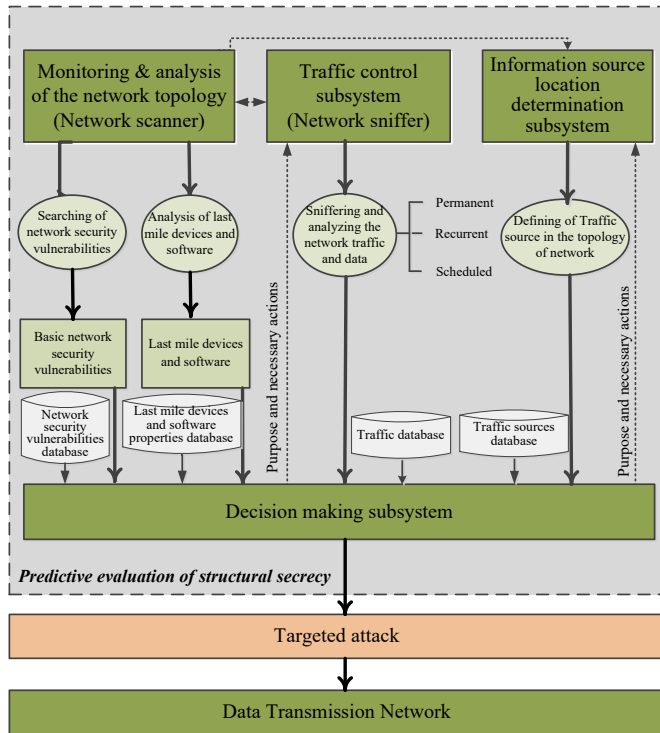


Fig. 1. The model of the targeted attack.

Network structure disclosing is provided by representation of data transmission network elements in the form of graph

vertices. The information links between them are presented as branches of the graph.

As a result, a structure of the graph corresponding to a stage of a technological process, which is implemented in a data transmission network, is formed.

Knowing typical structures corresponding to the main technological processes, the attacker forms a base of graph-templates. Then he (she) compares the observed structure of the data transmission network with that of a typical graph-template. As a result of this comparison, the type and stage of the process to be implemented is determined.

Thus, by carrying out the actions presented in the model of the targeted attack (for transmission network structure disclosing), the attacker can fully determine the nature of the activity in the information infrastructure in which interaction is carried out through the data transmission network.

B. Algorithms for evaluating the probability of disclosing the data transmission network structure

The main algorithms for estimating the probability of disclosing the data transmission network structure are (1) the algorithm for recognizing the data network structure and (2) the algorithm for estimating the structural secrecy of the data transmission network [24].

The initial data for the algorithm for recognizing the data transmission network structure are typical structures corresponding to the main technological processes.

These structures are formed by the network security administrator (possibly together with business analysts). The *graph-implementation* refers to the network under investigation. The *graph-template* refers to a graph included in a set of typical diagrams for organizing a technological process on the network.

The algorithm for recognizing the data transmission network structure is based on representing the graph in form of an adjacency matrix. It includes the following four main stages.

Stage 1. Finding paths and cycles on the graph-implementation using the depth search method [29].

Stage 2. Checking the equality of the number of vertices, the number of paths (cycles) in the graph, and the equality of degrees. A substitution matrix is generated from the cycles to be checked.

Stage 3. Finding vertices that are not in the test cycles. Checking whether the adjacency and equality relationship is maintained.

Stage 4. Addition to the substitution and output of the recognition result.

At the same time, the attack success depends mostly on the success of disclosing the structure of the data transmission network, since the network topology analysis is the first step in the targeted attack model discussed above.

The algorithm for evaluating the structural secrecy of a data transmission network can be applied both to individual elements of the data transmission network and to the network as a whole (Fig. 2).

The initial data of the algorithm is the results of the network scanning. Consider the operation of this algorithm.

Each of the terminals (terminal devices) transmits IP-packets with a rate λ_{ij} . This intensity is calculated in the module 4 by the formula

$$\lambda_{ij} = \frac{N_{ij}}{t_{session}}, \quad (1)$$

where N_{ij} is a number of IP-packets between corresponding pairs; $t_{session}$ is a time of the TCP (UDP) connection between terminals.

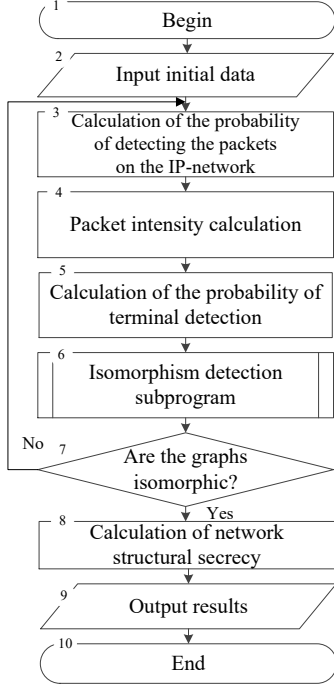


Fig. 2. The algorithm for evaluating the structural secrecy of a data transmission network.

In the module 5, the probability $P_i(t)$ that at the i -th terminal at a given time t the process will be implemented at least once is calculated. To do this, the following expression is used:

$$P_i(t) = 1 - \exp\left(-\sum_{j=1}^{d_i} \left(\int_0^t \lambda_{ij} \cdot p_{ij}(x) dx\right)\right), \quad (2)$$

where $p_{ij}(t)$ is the probability of detecting the IP-packets of corresponding pairs; d_i is a number of terminals interconnected with the i -th terminal and operated in the mode of transmitting and receiving IP-packets.

The module 6 implements a procedure for determining whether the graph-implementation belongs to one of the graph-templates. These actions are based on the procedure of recognizing the isomorphism of an occurrence of weighted graphs. The graph-implementation results from statistical modeling of the data transmission network. The second graph is a graph-template.

Upon successful execution of the graph isomorphism recognition procedure, the index Q_{ik} of structural secrecy of the k -th element relative to the i -th technological process is calculated using the following formula:

$$Q_{ik} = \frac{w_i(k)}{M}, \quad (3)$$

where $w_i(k)$ is a number of cases when the graph-implementation belongs to i -th graph-template at the actual draw of the k -th element; M is a total number of graph-templates. We assume that all graph-templates are available for the security administrator.

Thus, the presented algorithms ensure the recognition of the structure of the data transmission network through the probability of detection of the IP-network terminal and provide evaluation of the structural secrecy of the data transmission network.

IV. IMPLEMENTATION

The toolbox was developed for implementation of the offered approach to assess the probability of disclosing the data transmission network structure. As a programming language, C# on Microsoft .NET Framework was chosen. In future work, we plan to make this toolbox publicly available.

The program code for implementing the algorithm for recognizing the data transmission network structure is given in Listing 1.

```

internal Graph IsomorphicShuffling
{
    Graph graph = new Graph();
    int[] arT = new int[this.NodeCount];
    for (int index = 0; index < this.NodeCount; ++index)
        arT[index] = index;
    Graph.Shuffle<int>(arT);
    graph.InsertNodes(this.NodeCount);
    for (int index = 0; index < this.NodeCount; ++index)
    {
        foreach (Graph.eNode eNode in
            (IEnumerable<Graph.eNode>)
            this._nodes[arT[index]]._edgesFrom.Values)
            graph.InsertEdge(arT[this.PosFromId(eNode._idFrom)],
                arT[this.PosFromId(eNode._idTo)]);
    }
    return graph;
}
  
```

Listing 1. A code for implementing the algorithm for recognizing the data transmission network structure.

Input data is entered in the form of the adjacency matrix. The program code for implementation of initial data input is provided in Listing 2.

```

public void TestShuffle()
{
    Random rnd = new Random(10);
    int length = 100;
    int[] arT = new int[length];
    for (int index = 0; index < length; ++index)
        arT[index] = index;
    Assert.AreEqual(0, arT[0]);
    Assert.AreEqual(99, arT[99]);
    Graph.Shuffle<int>(arT);
    Assert.AreNotEqual(0, arT[0]);
    Assert.AreEqual(99, arT[99]);
    int num = 0;
    for (int index = 0; index < length; ++index)
        num += arT[index];
    Assert.AreEqual(length * (length - 1) / 2, num);
}
  
```

Listing 2. A code for implementation of initial data input.

The user interface is developed for convenience of interaction with the toolbox. The result is displayed as a message with negative or positive evaluation of the action.

V. EXPERIMENTAL EVALUATION

A fragment of the data transmission network included in the information infrastructure of the North-West Region Railway of the Russian Federation was considered for experimental evaluation of the proposed approach. This fragment contains 6 railway stations.

Fig. 3 shows the structure of the selected data transmission network fragment. The network has six nodes, where terminals (participants of the information exchange) are located: X1, ..., X6. The nodes are interconnected by data channels designated as e1, ..., e9. The graph presented in Fig. 3, plays the role of the graph-implementation. The graph-template obtained from the operation of the algorithm for recognizing the data transmission network structure is depicted in Fig. 4.

The graph-template also has six nodes: Y6, ..., Y6. It also has nine arcs connecting the nodes of the graph: e1, ..., e9. However, as can be seen from the comparison of Fig. 3 and Fig. 4, the set of arcs in the graph-implementation does not coincide with the set of arcs in the graph-template.

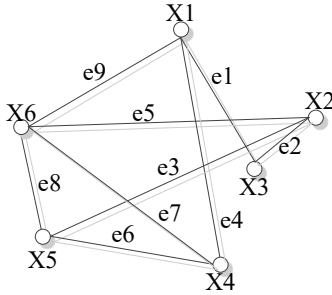


Fig. 3. The graph-implementation for a fragment of the data transmission network.

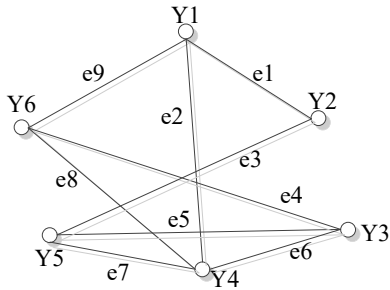


Fig. 4. The graph-template for a fragment of the data transmission network.

The results of calculating the IP-network terminal detection probability, obtained using (1) and (2) and presented as probability dependencies on the duration of the computer attack, are shown in Fig. 5. As it can be seen from Fig. 5, the probability of detecting each terminal, when the attack duration is sufficiently long (400 minutes), tends to one. At the same time, with a small (100 minutes) or average (200 minutes) attack duration, the probabilities of detecting terminals differ from each other. They depend on the existing data network structure.

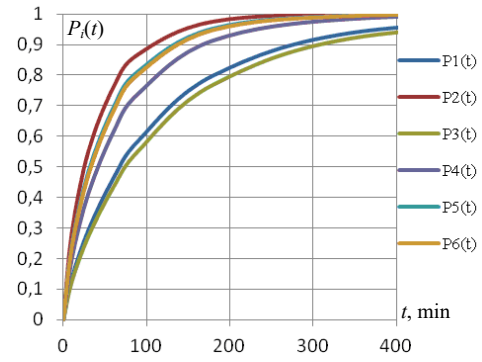


Fig. 5. Dependencies of the IP-network terminal detection probabilities on the duration of the computer attack.

Dependencies of probabilities of disclosing the data transmission network structure on time and number of graph-templates are presented in Fig. 6 (N is equal to 1, 2, and 5) and Fig. 7 (N is equal to 10, 20, and 30).

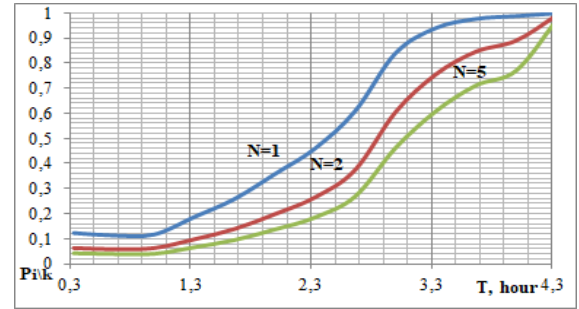


Fig. 6. Probabilities of disclosing the data transmission network structure at $N = 1, 2$, and 5.

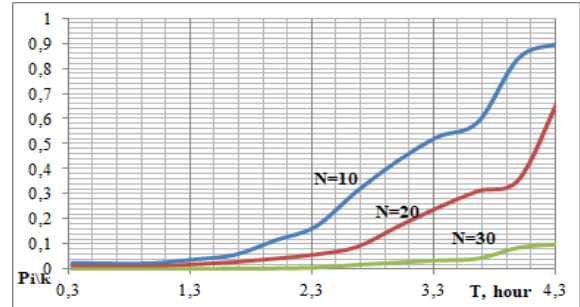


Fig. 7. Probabilities of disclosing the data transmission network structure at $N = 10, 20$, and 30

Results depicted in Fig. 6 and Fig. 7 show that an increase in the number of graph-templates results in a significant reduction in the probability of disclosing the network structure. Thus, it can be considered that the increase of graph-templates should be considered as a new way of protecting against targeted attacks, which is justified by the approach proposed.

VI. CONCLUSION

The paper considered the approach based on graph theory to evaluating the probability of disclosing the structure of the data transmission network when the attacker implements targeted attacks. The conceptual model of targeted attack of the

attacker was presented. This model shows that the corresponding pairs in the IP-address space refer to unmasking features. Analysis of such pairs allows the attacker to disclose the network structure, implement a computer attack and damage the information infrastructure. This determines the importance of the task of evaluating the probability of disclosing the data transmission network structure under implementing targeted attacks.

The developed algorithms for estimating the probability of disclosing the data transmission network structure consist of the algorithm for recognizing the data transmission network structure and the algorithm for evaluating the structural secrecy of the network. The first algorithm is an algorithm of one of the procedures included in the second algorithm. The idea of evaluating the structural secrecy of the network is to check the isomorphism of the graph-implementation and the graph-templates corresponding to technological processes. The isomorphism of both graphs corresponds to the low structural secrecy of the network. On the contrary, if the graphs are not isomorphic, it increases the structural secrecy of the network, as the attacker cannot get the correct representation of the technological processes.

Experimental evaluation of the proposed approach on the developed toolbox demonstrated the validity of the approach. For the fragment of the active data transmission network, the dependence of the probability of detection of terminals on the duration of the targeted attack and the results of calculation of the structural secrecy of the network were obtained.

Further directions of research are linked with the implementation of the proposed method in the software-tool environment of security monitoring system for large-scale transmission networks of the North-West Region Railway of the Russian Federation.

ACKNOWLEDGMENT

Research is carried out with support of Ministry of Education and Science of the Russian Federation as part of Agreement No. 05.607.21.0322 (identifier RFMEFI60719X0322).

REFERENCES

- [1] C. Tankard, "Advanced persistent threats and how to monitor and deter them", *Network Security*, vol.2011, no.8, pp.16–19, 2011.
- [2] C.-M. Chen, G.-H. Lai, D.-W. Wen, "Evolution of Advanced Persistent Threat (APT) Attacks and Actors", *Communications in Computer and Information Science*, vol. 1013, Springer, Singapore, pp.76–81, 2019.
- [3] J. Navarro, "Modelization and Identification of Multi-step Cyberattacks in Sets of Events", Ph.D. Dissertation, Université de Strasbourg, 2019.
- [4] W.L. Chu, C.J. Lin, K.N. Chang, "Detection and Classification of Advanced Persistent Threats and Attacks Using the Support Vector Machine", *Applied Sciences*, vol.9, no.21, pp.4579, 2019.
- [5] J.E. Rubio, R. Roman, C. Alcaraz, Y. Zhang, "Tracking advanced persistent threats in critical infrastructures through opinion dynamics", in *Computer Security. ESORICS 2018, Lecture Notes in Computer Science*, vol. 11098. Springer, Cham, pp.555–574, 2018.
- [6] L. Huang, Q. Zhu, "Adaptive strategic cyber defense for advanced persistent threats in critical infrastructure networks", *ACM SIGMETRICS Performance Evaluation Review*, vol.46, no.2, pp.52–56, 2019.
- [7] I. Friedberg, F. Scopik, G. Settanni, R. Fiedler, "Combating advanced persistent threats: From network event correlation to incident detection", *Computers and Security*, vol.48, no.C, pp.35–57, 2015.

- [8] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", *Computers and Security*, vol.28, no.1-2, pp.18–28, 2009.
- [9] M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, "Network anomaly detection: methods, systems and tools", *IEEE Communications Surveys & Tutorials*, vol.16, no.1, pp. 303–336, 2013.
- [10] M. Li, "A New Detection Method of Network APT Based on Big Data Analysis", in *Proceedings of the 2018 3rd International Workshop on Materials Engineering and Computer Sciences (IWMECS 2018)*, Atlantis Press, 2018.
- [11] M. Marchetti, F. Pierazzi, M. Colajanni, A. Guido, "Analysis of high volumes of network traffic for advanced persistent threat detection", *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol.109, no.P2, pp.127–141, 2016.
- [12] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, B. Stiller, "An overview of IP flow-based intrusion detection", *IEEE Communications Surveys & Tutorials*, vol.12, no.3, pp. 343–356, 2010.
- [13] N. Villeneuve, J. Bennett, "Detecting APT activity with network traffic analysis", *Trend Micro Incorporated Research Paper*, pp.1–15, 2012.
- [14] D. Zhao, I. Traore, B. Sayed, W. Lu, Sh. Saad, A. Ghorbani, D. Garant, "Botnet detection based on traffic behavior analysis and flow intervals", *Computers and Security*, vol.39, pp.2–16, 2013.
- [15] F. Anjum, D. Subhadrabandhu, S. Sarkar, "Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols", in *2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484)*, vol.3, pp. 2152–2156, 2003.
- [16] I. Kotenko, "Active Vulnerability Assessment of Computer Networks by Simulation of Complex Remote Attacks," in *2003 International Conference on Computer Networks and Mobile Computing. Proceedings. IEEE Computer Society*, pp.40–47, 2003.
- [17] I. Kotenko, M. Stepashkin, E. Doynikova, "Security analysis of information systems taking into account social engineering attacks," in *Proceedings of 19th International Euromicro Conference on Parallel, Distributed, and Network-Based Processing*, pp.611–618, 2011.
- [18] I. Kotenko, A. Chechulin, "Computer attack modeling and security evaluation based on attack graphs," in *Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS 2013)*, pp.614–619, 2013.
- [19] I. Kotenko, E. Doynikova, "Security assessment of computer networks based on attack graphs and security events," *Lecture Notes in Computer Science*, vol.8407, pp.462–471, 2014.
- [20] E. Doynikova, I. Kotenko, "Improvement of Attack Graphs for Cybersecurity Monitoring: Handling of Inaccuracies, Processing of Cycles, Mapping of Incidents and Automatic Countermeasure Selection," *SPIIRAS Proceedings*, Issue 2(57), 2018.
- [21] J.R. Johnson, E.A. Hogan, "A graph analytic metric for mitigating advanced persistent threat", in *Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics (ISI 2013)*, IEEE, pp.129–133, 2013.
- [22] G.S. Bopche, B.M. Mehtre, "Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks", *Computers and Security*, vol.64, pp.16–43, 2017.
- [23] A.D. Kent, L.M. Liebrock, J.C. Neil, "Authentication graphs: Analyzing user behavior within an enterprise network", *Computers and Security*, vol.48, pp.150–166, 2015.
- [24] J. Kobler, U. Schöning, J. Torán, "The graph isomorphism problem: its structural complexity", Springer Science & Business Media, 2012.
- [25] L.P. Cordella, P. Foggia, C. Sansone, M. Vento, "A (sub) graph isomorphism algorithm for matching large graphs", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.26, no.10, pp.1367–1372, 2004.
- [26] P. Foggia, C. Sansone, M. Vento, "A database of graphs for isomorphism and sub-graph isomorphism benchmarking", in *Proceedings of the 3rd IAPR TC-15 International Workshop on Graph-based Representations*, pp.176–187, 2001.
- [27] U. Redmond, P. Cunningham, "Subgraph isomorphism in temporal networks", in *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM '13)*, pp.1451–1452, 2013.
- [28] Custom Defense Against Targeted Attacks, A Trend Micro, 2014.
- [29] Sh. Even, "Graph algorithms", Cambridge University Press, 2011.