A Study of Cyber Attack Behavior based on Algebraic Topology

Zhang Xiaoyu, Yan Huaizhi* and Liu Zhenb

School of Computing, Beijing Institute of Technology, Beijing, 100081, China

Corresponding author’s e-mail: *yhzhi@bit.edu.cn, b3120185535@bit.edu.cn

Abstract. It is inevitable that serious damage will occur once the hosts suffer from cyberattack. Therefore, the study of cyberattacks has become indispensable in the field of cyber security. Host-oriented cyberattacks consist of a series of atomic attacks attacking system objects and metrics on atomic attacks can quantitatively describe the behavior of cyber attacks. When the atomic attack behavior constitutes a manifold topological space, host-oriented assessment of the effects of a cyberattack can be computed using an algebraic topology. The concepts of manifold and other spaces in algebraic topology can be used to model and analyze the system composed of many elements. Therefore, by handling the relationships between metrics appropriately (e.g., complex mappings), the topological space of attack scenarios is constructed. This paper uses a cellular manifold to show the geometric structure of cyberattack behaviors. In this solution, we select the metrics depicting the cyber attack behavior and clear their dependence through the construction of cyberattack behavior sequence graph, and then put forward the cyberattack behavior model based on the relationship between metrics. WannaCry ransomware attack is analyzed by applying our model, which provides a new idea for quantifying cyberattack.

1. Introduction

The cyber attack modelling technique using the visual language of graph/tree/net depicts attack scenarios for multiple hosts in a network. As an example, the attack graph-based cyber attack modelling technique explains why attacks occur and highlights potential attack identification and weakness discovery [1, 2]. However, both the original attack graph and various improved attack graphs use hosts as nodes and topological relationships between hosts as relationships between nodes [3]. It is not directly applicable to the study of host-oriented network attack behaviour. Host-oriented attack behaviour research is a more granular, host-level study that takes the host system object of the attack as the nodes, the relationships between system objects as relationships between nodes.

Quantitative calculations of the effect of an attack require metrics that can quantify the effect, and different attack scenarios require different metrics [4]. However, existing attack graph cannot comprehensively identify the data to be collected and the metrics to be defined for different attack scenarios [5]. The attack graph shows all the paths by which an attack exploits the device vulnerabilities or weaknesses to reach the attack target [6], and presents attack information such as vulnerability information, network topology, application information, and prerequisites for executing the attack [7, 8]. Our cyberattack model based on security data metrics is more concerned with what kind of security data is collected at which node than the prerequisites highlighted by the attack graph. For this purpose, we propose an attack behaviour sequence graph to analyze the system objects affected by each step of the attack, collect security data related to the system objects, and finally construct quantitative metrics based on the security data.

While security metrics can describe the process of an attack, it is a challenge to organize these metrics for calculating the effect of an attack. Most of the existing metric-based cyber security...
assessment methods take Analytic Hierarchy Process (AHP), which involves human factors in both the assessment of cyber security and the measurement of attack effects [9, 10]. In order to fully and objectively quantify the effect of the attack, Hu [11] proposes to use manifolds with a metric structure in the algebraic topology. A manifold is a space that locally has the nature of Euclidean space. Hu states that the effect of an attack is the cumulative sum of the calculus of the behaviours over the manifold behaviour path. While the paper gives a detailed method for calculating the attack effect, it does not detail how to construct manifolds.

Then the problem of metrics used to calculate the effect of an attack translates into the problem of constructing manifolds using indicators. Since a simplicial complex is a good tool for analysing complex systems that contain multiple interacting elements [12], and a simple complex that meets certain conditions is a manifold. To obtain a manifold we propose to construct geometric spaces (simple complexes) of security metrics using knowledge of algebraic topology, and finally to obtain the topological relation model of metrics (a manifold). Since geometry is the basis of algebra, the construction of geometric topologies between indicators helps in the study of effects calculations for cyberattack behaviour. Since geometry is the basis of algebra, constructing a geometric topology between metrics facilitates the study of calculation of attack effects.

There are a number of papers on data acquisition or modelling of cyber attack behavior [13–15], but they do not focus on the data relationships and geometric space relationships of the metrics, which is what we are interested in.

The rest section of this paper is organized as follow. In Section 2, we provide definitions of the terms involved in the Attack Behavior Sequence Graph. In Section 3, we give the process of analyzing cyber attack: creating an attack behavior sequence graph, analyzing the metrics of the attack scenario, and constructing the manifold of the metrics. In Section 4, we show the process and results of WannaCry attack with our model. At last, we give our conclusion and the future work in Section 5.

2. Preliminary
In this section, we give relevant definitions (security metrics, atomic attack, attack object) for the analysis of host-oriented cyberattack behavior. In addition, we give knowledge and necessary definitions of the algebraic topology involved in the analysis of cyberattack behaviors. In order to better understand the model for evaluating the cyberattack behavior proposed in this paper, relevant proof conditions from simplicial complex to manifold are also given.

**Definition 1**: An attack object is an entity that is the target of an atomic attack. From the perspective of hosts, there are a limited number of entities that are often targeted. The attack objects in this paper mainly include files, processes, Windows registry and network packets.

**Definition 2**: An atomic attack [16], is an operation on an attack object. For each type of attack object the following atomic attacks are available. For example, create executable files, modify files, delete files. The attack objects and atomic attacks are not limited to those give. When the attack scenario is a ransomware attack, the file object adds an encryption operation.

**Definition 3** A security metric in this paper focuses on the measured raw data, which is the effect of an atomic attack or the characterization of an attack object. This data is usually collected from security devices (firewalls, etc.) or from logs. We refer to security data that evaluates the effect of a cyber attack as metrics, which is different from the traditional sense of the term.

The metrics should meet the following conditions:
- metrics should be detectable or quantifiable, which are generally value and existence [17].
- the value of metrics should be affected by atomic attacks and change accordingly.

**Definition 4** A abstract simplicial complex is a set $A$ together with a collection $\Delta$ of subsets of $A$ such that if $X \in \Delta$ and $Y \subseteq X$, then $Y \in \Delta$, where the elements of $A$ are the vertices of $\Delta$.

A security metric is abstracted as the element of the subset of $A$. For a specific attack scenario, if the set of security metrics consist of $a, b, c$, then the collection $\{\{a\}, \{b\}, \{c\}\}$, the collection $\{a, b\}, \{a, c\}, \{b, c\}, \{a, \}, \{b\}, \{c\}$ and the collection $\{\{a, b, c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a\}, \{b\}, \{c\}$ are all
The construction process of abstract simplicial complex is illustrated with an algorithm in the next section.

### 3. The proposed modelling method of cyber attack

The analysis process of cyber attack behavior mainly contains the construction of cyber attack behavior sequence graph and geometric model of security metrics. The cyber attack behavior sequence graph analyzes each step of attack behavior according to certain rules, and then forms a coherent behavior sequence. In the process of constructing the cyber attack behavior sequence graph, the available metrics are identified based on each node. Finally, the geometric model of metrics is constructed. More security metrics indicate a higher dimensionality of their data space. Obviously, it is hard to compute using high dimensional data space. To solve this problem, we construct attack behavior sequence graph to analyze attack objects and atomic attacks of an attack scenario.

In the attack behavior sequence graph, we consider the attacks carried out by the attacker and the objects affected by the attack, i.e., atomic attacks and attack objects. Cyberattacks can be categorized according to atomic attack so we use atomic attacks to analyze how an attacker exploits objects to reach the results. It is important to explain that we are not concerned with the prerequisites and exploits of each attack step, but only with the objects affected by the attack. This is different from the attack graph.

The cyber attack behavior sequence graph is defined as a directed graph. And it is expressed by a tuple of the form \( \text{ASG} = (I, O, R, A) \) where \( I \) represents the initial attack object, \( O \) represents the target reachable object, and \( A \) represents the atomic attack. The method of determining the granularity of an atomic attack is that the anomalous operation is not devided, and the types of atomic attacks are given in detail in the Def 2. Attacks on different attack objects are treated as different atomic attacks. The initial attack object is the source of attack process, which is usually a payload such as a virus, Trojan, or executable file. The type of attack object is given in detail in Def 1.

#### 3.1. the Constraction of Metric Set

The selection of correct and reasonable security metrics is an important basis for assessing cybersecurity. The scientific feasibility of the selection of security metrics will have a direct impact on the correctness and reasonableness of the results of the use of the model. Therefore, in the process of the selection of metric set, the security metrics must be selected scientifically and reasonably.

We define the set of security metrics as a metric set. See Def 2 for more details.

#### 3.2. The Geometric of Cyber Attack

Since the cyber behavior can be described by metrics, in this section we abstract the metric set into abstract simplicial complex according to the dependencies of metrics, and get the simplicial complex.

Construct the Abstract Simplicial Complex We can create distinct sets according to the dependencies and the collection of these sets is an abstract simplicial complex. Above all we need to specify the dependency mapping relation between metrics. The relationship between metrics are dependency mapping relationship and non-dependency mapping relationship.

Depending on the dependency mapping relationship between metrics, we can create the collection \( \Delta \) and make \( \Delta = \emptyset \) initially. By following the steps, we can get the final result \( \Delta \).

---

**Algorithm 1 Construction of Abstract Simplicial Complex**

| Input: metric set \( \Lambda \) |
|---------------------------------|
| Output: collection \( \Delta \) |

1. Each metric is incorporated into the \( \Delta \) as a single set, so there is \( \Delta = \Delta \cup \{i_n\} \)
2. For any two elements \( \{i_n\} \) and \( \{i_m\} \) in collection \( \Delta \), if there is no dependency mapping relationship between metrics \( i_n \) and \( i_m \), then \( \Delta = \Delta \cup \{i_n, i_m\} \)
3. For any three elements \( \{i_n, i_m\}, \{i_j, i_k\} \) and \( \{i_l, i_m, i_k\} \) in \( \Delta \), if there is no dependencies mapping relationship among \( i_n, i_j \) and \( i_l \), then \( \Delta = \Delta \cup \{i_n, i_j, i_k\} \).
4. For any four elements \(\{i_n, i_m, i_{m'}, i_{m''}\}\), \(\{i_n, i_{m'}, i_{m''}, i_{m'''}\}\), \(\{i_n, i_{m'}, i_{m''}, i_{m'''}\}\) and \(\{i_n, i_{m'}, i_{m''}, i_{m'''}\}\) in \(\Delta\), if there is no dependency mapping relationship among \(i_n, i_{m'}, i_{m''}\) and \(i_{m'''}\), then \(\Delta = \Delta \cup \{i_n, i_{m'}, i_{m''}, i_{m'''}\}\).

5. Similarly, for any \(T\) elements in \(\Delta\), if thereon dependency mapping relationship among any metrics, then \(\Delta = \Delta \cup \{i_{t_1}, i_{t_2}, \ldots, i_{t_T}\}\)

6. **Return** collection \(\Delta\)

The steps of Algorithm 1 is essentially the construction procedure of poset. As a matter of fact, the vertex set of the abstract simplicial complex \(\Delta\) is the metric set, and the elements are a subset of the simplices. \(\Delta\) can be represented as the collection of simplices, denoted by \(\Delta = \{A\}_{A \in A} = \{i_{n_{a_1}}, \ldots, i_{n_{a_N}}\}\), where \(A\) is the vertex set of a simplex i.e. metrics.

Geometric Simplicial Complex - the Geometric Realization of Abstract Simplicial Complex

Abstract simplicial complex only embodies the data relation between metrics without considering the topological structure formed by metrics, so that it cannot be used for calculation. It is necessary to study the topological relation of data space through the geometric realization.

The isomorphic geometric simplicial complex corresponds to the same abstract simplicial complex. The simplest example is the complex with two edges connecting two vertices and the complex with one edge connecting two vertices. In order to avoid that the geometric simplicial complex derived from the geometric realization is not unique, we specify that the simplices in the collection \(\Delta\) only appears once when the geometric realization of the abstract simplicial complex \(\Delta\). It ensures that the geometric realization is unique in the sense of linear isomorphism. And the obtained geometric simplicial complex is the simplest case. The detailed understanding is further illustrated in the following case study.

In this article, we use the combinatorial data provided by an abstract simplicial complex and construct a topological space by gluing simplices together [18]. If an abstract simplicial complex \(\Delta = \{A_{\alpha}\}_{A_{\alpha} = \{i_{n_{a_1}}, \ldots, i_{n_{a_N}}\}}\), then there is a topological space determined by the set of equivalence classes as (1).

\[
|A| = \bigcup_{A_{\alpha} \in \Delta} \sigma_{\alpha}^N
\]  

(1)

The construction of topological space is a process of quotient topology solution, and the resulting quotient space is homeomorphic to a geometric simplicial complex formed by vertices in \(\mathbb{R}^N\). A geometric simplicial complex can be constructed by starting at any vertex and then gluing simplex one by one in any order. The only thing that needs to be satisfied is to ensure that all the suitable subsimplices of a simplex have been glued to this point according to the equivalence condition of (1).

So far, \(\Delta_A\) is the quotient space homeomorphic to the subspace of \(\mathbb{R}^N\), and the relation between the combinatorial data \(\Delta_A\), the collection of sets of metrics, and the topological space determined by the union of simplex \(\sigma_{\alpha}^N\) is distinguished by \(|\Delta_A| = \bigcup_{A_{\alpha} \in \Delta_A} \sigma_{\alpha}^N\). The abstract simplicial complex of cyber attack effect are constructed into geometric simplicial complex \(|\Delta_A|\) with geometric significance.

The description of cyber attack has changed from combinatorial data to topological data, and the study of cyber attack behavior is abstracted into topological space study in topology.

**Manifold - the Simplicial Meets Some Conditions**

Next, we demonstrate step by step that the simplicial complex \(|\Delta_A|\) is cellular complex, regular cellular complex and manifold.

According to the definition of cell and simplex [19, 20], an open cell is a cell. Any finite \(m\)-simplicial complex can be decomposed into open simplices with dimensions less than \(m\). Similarly, the finite simplicial complex of higher dimensions can be decomposed into a finite number of open cells.

Due to the finite number of metrics, the topological space \(|\Delta_A|\) is compact. According to the lemma. Also according to the lemma the topological space \(|\Delta_A|\) is hausdorff space [21].

These two points meet the prerequisite for a cellular complex - a compact Hausdorff space. So that the simplicial complex \(|\Delta_A|\) is a cellular complex by definition of cellular complex [19]. In fact, the concept of cellular complex is an extension of simplex and complex in algebraic topology. The
convexity set constraint of simplex was extended to define the cell and the cellular complex. A $n$-cell
is a space homeomorphic to an $n$-simplex [22].

According to the definition of the regular cellular complex [19], each cell is open. As mentioned
earlier the simplicial complex $|\Delta_1|$ can be decomposed into many open simplices, which means
the homeomorphic mapping of a simplex is an open cell. At the same time, the boundary of $q$-open
simplex, i.e. $q$-closed simplex get rid of the inside, is subcomplex of simplicial complex $|\Delta_1|$ obviously.
So the simplicial complex $|\Delta_1|$ is clearly a regular cellular complex.

So far, we know that the effect of cyber attacks is geometrically a regular cellular complex $|\Delta_1|$ on
$\mathbb{R}^n$. Next, we continue to prove that the complex $|\Delta_1|$ is a manifold.

The necessary and sufficient condition for a simplicial complex to be a cellular manifold is as
follows[21]: for each simplex $s^q$, the linked complex $lk(s^q)$ is homeomorphic to sphere $S^{n-q-1}$ with
$n - q - 1$ dimension. For each simplex $s^q$ of $|\Delta_1|$, the linked complex is isomorphic to the link
lk$(s^q)$. So the necessary and sufficient condition for a simplicial complex to be a cellular manifold
turns into: the linked $lk(s^q)$ is homeomorphic to sphere $S^{n-q-1}$ with $n - q - 1$ dimension.

The $n$-complex obtained by the algorithm 1, we can get the following conclusions:

- The simplicial complex $|\Delta_1|$ is a pure complex.
- The simplicial complex $|\Delta_1|$ is nonsingular.

According to the above conclusion and [23], it can be proved that the cellular link of regular
cellular complex $lk(s^q)$ is homeomorphic to the $n - q - 1$-sphere or $n - q - 1$-closed ball. Every
face of $|\Delta_1|$ is nonsingular, so the link of every internal face is a sphere whereas the link of every
external face is a ball[23]. Moreover, the cell of regular cellular complex $|\Delta_1|$ is an open simplex, so
the cell link of regular cellular complex $|\Delta_1|$ is homeomorphic to the $n - q - 1$-sphere.

To sum up, the whole cyber attack occurs in the same topological space which is the manifold
formed by the data metric describing the cyber attack behaviors, denoted as $M$. The cyber attack
behavior model we constructed is a cellular manifold in combinatorial algebraic topology, which is
composed of many cells. And the measurement structure (such as Riemann measure) can be added to
this geometric structure, manifold, to calculate the measurement of cyber attack effects.

The cellular manifold reflects the relationship between the atomic attack measurement and the
whole cyber attack measurement very well. The whole cyber attack behavior is a partial combination
of atomic attack behavior, and atomic attack behavior can be listed in the form of combination. Many
nice characteristics of cellular manifold can be used to study the effects calculation of cyber attack
further, which lays a foundation for further research.

4. Case Study

The attack process of WannaCry ransomware is taken as an example to explain attack behavior
sequence graph and the geometric significance of security metrics in detail. The basic attack process of
WannaCry ransomware is shown in Fig.1. WannaCry ransomware is mainly divided into a worm
module and a ransomware module [24]. Corresponding to our modeling process, there are three steps
in case study.

![Figure 1 The attack process of WannaCry](image-url)
4.1. Build Cyber Attack Behavior Sequence Graph

By analyzing the collected operation data we identified the atomic attacks and the attack objects. And we constructed the cyber attack sequence graph of a host infected with WannaCry ransomware. WannaCry’s atomic attacks come in pairs with the object of action. They are shown in Table 1.

Table 1. Main atomic attacks and attack objects of WannaCry

| attack object | attack object     |
|---------------|-------------------|
| Files: wacy.exe | execute           |
| Files: taskche.exe | copy and rename  |
| Windows register: HKEY LOCAL MACHINE and HKEY CURRENT USER | write       |
| Processes: the database-related processes | close       |
| Files: shadow copies | delete    |
| Files: user files | encrypt      |
| Network packets: tcp packets | send and accept |

Fig. 2 shows six different paths with real or dashed lines of different thickness.

Figure 2. Cyber attack behavior sequence graph of WannaCry ransomware

4.2. Select metric Set

We screen out the corresponding metrics at the grey node in Fig 2. In ransomware module, the database-related processes and locks on files are terminated to prevent encryption and overwriting of files from being blocked and then files(*.*) are encrypted into files with the .wcry suffix. The attacker also deletes shadow copies so as to stop users restoring files from backup files. The ransomware module modifies the registry to ensure itself startup. Once the worm module is registered as a service, it starts to scan and send the connection request. The above describes attack behavior that act on grey nodes. Table 2 shows specific metrics and corresponding metric information. The metric set $A = \{IEP, NEP, IRM, NRM, ISC, NSC, IEF, NEF, NTSP \ | \phi_n, 0 < n < 5 \}$. Behaviors that ensure that the attack is successfully executed but do not have an effect can be omitted from the sequence.

Table 2. metrics and their detail information of WannaCry

| Name | Detailed Description | Type      | Corresponding Attack Object | Dependency Relation |
|------|----------------------|-----------|-----------------------------|---------------------|
| IEP  | Whether the processes are ended successfully | existence | The processes related to database and locks on files | $\phi_1$: $IEF \rightarrow NEP$ |
| NEP  | the Number of ended processes | value     |                             |                     |
4.3. Construct Geometric Model

Although the combinational data is quite large, the elements of the abstract simplicial complex are determined as long as the maximal simplex is determined. We only give the vertices of the maximal simplex. The vertices of maximal simplex depend on NTSP and any one metric of each mapping relation. There are total of 2^4 kinds of combinations. So the mathematical representation of the abstract simplicial complex \( \Delta_4 \) is a vertex set and subsets of the 2^4 maximal simplex. The vertices of each simplex are connected.

Since geometries higher than 3 dimensions are difficult to plot, here we describe only the geometric generation process of cyber attack behavior: the vertices of the maximal simplices are connected to each other to get a complex composed by 2^4 4-simplex. Then, starting from the common vertices of one 4-simplex each 4-simplex is ‘glued’ in turn. This yields the 4-simplicial complex \( \Delta_4 \). By the proof in 3.3, we know that this is a geometric 4-cellular manifold \( M \). The cellular manifold \( M \) is represented by 16 maximal simplices, and it is a local combination of these simplices. If the maximal simplex is expressed as \( \sigma_n \), then the cellular manifold is expressed as the maximal simplex and its subsimplex, i.e. \( M = \{\sigma_1, \sigma_2, \ldots, \sigma_{16}\} \).

The attack effect of an atomic attack is described by metrics, which is the ‘work’ required to get from one grey node to another in the attack behavior sequence graph. So we give the geometry of each grey node. By providing these geometries, it is convenient to add a measurement structure to the geometric structure to evaluate the degree of effect.

After adding the Riemann measurement to the manifold, the vertex-to-vertex distance is the geodesic on the manifold, which is the calculable[11]. The attack effect of an atomic attack can be expressed as \( E_i = f \times s, s = \int u^j g_j \, dt \), where \( f \) is the instantaneous force of the atomic attack and \( s \) is the geodesic connection, \( u^j \) is the tangent vector of a point and a function of time \( t \), \( g_j \) is instantaneous covariant basic vector at the point position at time \( t \). The attack effect of an atomic attack can be denoted by \( E = \sum_i E_i \).

As can be seen from the ASG, WannaCry attack is divided into six attack paths. The metric subsets of these paths are \( A_1 = \{\text{ISC, NSC}\}, A_2 = \{\text{IEP, NEP, IEF, NEF}\}, A_3 = \{\text{IRM, NRM}\}, A_4 = \emptyset, A_5 = \emptyset, A_6 = \{\text{NSMBP}\} \). The simplicial complexes corresponding to these six metric subsets are all the subcomplex of \( M \) and also cellular manifolds. Table 3 shows the geometric models and their meanings of the effects of atomic attacks on different paths. The atomic attacks on Path 4 and Path 5 donnot materially affect the hardware and software services, but merely pop up the extortion screen up and provide the address for ransom payment. So the corresponding metrics and geometric model were empty sets. The attack effect of Wannacry is expressed as

\[
E = \int (f_1u_1g_{j_1} + f_2u_2g_{j_2} + f_3u_3g_{j_3} + f_6u_6g_{j_6}) \, dt
\]

Table 3. The metrics and corresponding meaning of WannaCry

| Path  | Indicators | Maximal simplicial** | Simplicial Complex | the meaning of simplicial complex |
|-------|------------|----------------------|--------------------|---------------------------------|
| Path 1| ISC, NSC   | two points, ISC and NSC | the geometry model for attack effect caused by deleting shadow copies |
| Path 2| IEP, NEP, IEF, NEF | the plane surrounded by segment | the geometry model for attack effect caused by ending database-related processes and encrypting files |
| Path 3| IRM, NRM   | two points, IRM and NRM | the geometric model for attack effect caused by modifying register |
| Path 6| NSMBP      | one point, NSMBP | the geometric model for attack effect caused by sending TCP packets |

**The abstract simplicial complex is the collection of maximal simplices and their subsets. 
5. Conclusion
The integral of the attack instantaneous force and the geodetic can be used to calculate the attack effect, but only if the topological space where the attack scenario is located is a manifold. In order to prove this premise, we determine different metrics based on different network attack behaviors and construct cyber attack behavior sequence graph with atomic attack as the edge and the target as the node. Furthermore, the complicated description problem of cyber attack behavior is transformed into algebraic topology problem step by step. The model is a cellular manifold. The main contribution of our work are as follow:

(i) use initial object, atomic attack and targeted object to analyze cyber attack behaviors;
(ii) present a new model which quantifies and visualizes cyber attack behavior by using algebraic topology knowledge. It is revealed that the geometric meaning of the whole cyber attack behavior is a cellular manifold and the subcomplex of the manifold is the geometric model of atomic attacks. Our model is applied to analyze WannaCry attack, and the geometric model of its metrics is presented and the calculation of attack effects at last. We put forward a new idea for the study of cyber attack behaviors.

In the future work, we will consider the reduction of unnecessary path representation, the refine of attack behavior sequence graph, and the number of selected metrics reduction according to the calculation requirements of different attack behaviors. We treat these questions as open questions for this work.

Acknowledgments
This work The National Key Research and Development Program of China(No.2016YFC1000301)

References
[1] Al-Mohannadi H, Mirza Q, Namanya A, Awan I, Cullen A, Disso J. Cyber-Attack Modeling Analysis Techniques: An Overview. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW): IEEE; 2016-2016, p. 69–76.
[2] Ayrour Y, Raji A, Nassar M. Modelling cyber-attacks: a survey study. Network Security 2018;2018(3):13–9.
[3] Barik MS, Mazumdar C. A Graph Data Model for Attack Graph Generation and Analysis. In: Martínez Pérez G, editor. Recent trends in computer networks and distributed systems security: Second international conference, SNDS 2014, Trivandrum, India, March 13-14, 2014, proceedings / Gregorio Martínez Pérez [and three others] (eds.). Heidelberg: Springer; 2014, p. 239–250.
[4] Miani RS, Cukier M, Zarpelão BB, Souza Mendes L de. Relationships between information security metrics. In: Sheldon F, editor. Eight Annual Cyber Security and Information Intelligence Research Workshop: Federal Cyber Security R & D Program Thrusts January 8-10, 2013. New York, NY: ACM; 2013, p. 1.
[5] Sheyner O, Haines J, Jha S, Lippmann R, Wing JM. Automated generation and analysis of attack graphs. In: 2002 IEEE symposium on security and privacy: IEEE Comput. Soc; 2002, p. 273–284.
[6] Angelini M, Bonomi S, Lenti S, Santucci G, Taggi S. MAD: A visual analytics solution for Multi-step cyber Attacks Detection. Journal of Computer Languages 2019;52:10–24.
[7] Kaynar K. A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications 2016;29:27–56.
[8] Lallie HS, Debattista K, Bal J. Evaluating practitioner cyber-security attack graph configuration preferences. Computers & Security 2018;79:117–31.
[9] Wilamowski G, Dever J, Stuban S. Using Analytical Hierarchy and Analytical Network Processes to Create Cyber Security Metrics. Defense ARJ 2017;24(2):186–221.
[10] Zaburko J, Szulżyk-Cieplak J. Information security risk assessment using the AHP method. IOP Conf. Ser.: Mater. Sci. Eng. 2020;710(1):12036.
[11] Hu C. Calculation of the Behavior Utility of a Network System: Conception and Principle. Engineering 2018;4(1):78–84.

[12] Salnikov V, Cassese D, Lambiotte R. Simplicial complexes and complex systems. Eur. J. Phys. 2019;40(1):14001.

[13] Shameli-Sendi A, Dagenais M, Wang L. Realtime intrusion risk assessment model based on attack and service dependency graphs. Computer Communications 2018;116:253–72.

[14] Sandoval JE, Hassell SP. Measurement, identification and calculation of cyber defense metrics. In: 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE: IEEE; 2010 - 2010, p. 2174–2179.

[15] Yao L, Dong P, Zheng T, Zhang H, Du X, Guizani M. Network security analyzing and modeling based on Petri net and Attack tree for SDN. In: 2016 International Conference on Computing, Networking and Communications (ICNC): IEEE; 2016 - 2016, p. 1–5.

[16] Zimba A, Chen H, Wang Z. Bayesian network based weighted APT attack paths modeling in cloud computing. Future Generation Computer Systems 2019;96:525–37.

[17] Kotenko I, Doynikova E. Selection of countermeasures against network attacks based on dynamical calculation of security metrics. Journal of Defense Modeling & Simulation 2018;15(2):181–204.

[18] McCleary J. A first course in topology: Continuity and dimension / John McCleary. Providence, RI: American Mathematical Society; 2006.

[19] Kozlov DN. Combinatorial algebraic topology. Berlin, New York: Springer; 2008.

[20] Jiang B. Homology theory. Peking: Peking University Press; 2007.

[21] Munkres JR. Elements of Algebraic Topology. Boulder: Chapman and Hall/CRC; 2018.

[22] Frank AU, Kuhn W. Cell Graphs: A Provable Correct Method for the Storage of Geometry 1986.

[23] Jean Gallier. Chapter 7 Basics of Combinatorial Topology; Available from: https://www.cis.upenn.edu/~cis610/complex1.pdf.

[24] Symantec. Ransom.Wannacry; 2017.