Review on the Application of Knowledge Graph in Cyber Security Assessment

Kai Zhang¹, Jingju Liu¹,*
¹ College of Electromagnetic Countermeasure, National University of Defense Technology, Hefei, China
*Corresponding author e-mail: jingjul@aliyun.com

Abstract. The development of artificial intelligence technology has advanced by leaps and bounds and made significant progress in many areas. Many researchers have begun to apply artificial intelligence technology to the cyber security domain. Knowledge graphs can describe the concepts, entities and their relationships in the objective world in a structured way. Applying knowledge graph to the cyber security domain can organize, manage, and utilize massive amounts of information in cyberspace in a better way. In this paper, the common cyber security assessment models and their shortcomings is summarized, the research progress of ontology-based knowledge representation is discussed, thus leading to a conclusion that ontology-based knowledge representation can completely and accurately represent the complex knowledge of heterogeneous systems in the cyber security domain. Then we introduce the concept of knowledge graph, summarize the application progress of knowledge graphs in the cyber security domain, and discuss directions of future research.

1. Introduction
With the development of information technology, cyber-attack incidents occur frequently, with the attack methods becoming increasingly complex, intelligent, and diversified. The cyber security-related data generated on the network has experienced explosive growth. These data are diverse, heterogeneous, and fragmented, making it difficult for cyber security managers to quickly find the information they need. It is a major problem that how to effectively analyze, mine and correlate massive data and information in the cyber security domain.

As the cyber security situation increasingly complex, researchers have proposed a variety of cyber security assessment and analysis models, such as attack graph model[1], attack tree model[2], Petri net model, and so on. They intend to use these models to actively analyze the vulnerability in the network, and then take measures to reduce network risks based on the results of the analysis. However, in the face of large-scale networks and massive data, the existing methods cannot meet the actual needs in terms of knowledge representation and reasoning. The knowledge graph for cyber security provides a new solution to the above problem.

The knowledge graph for cyber security uses the ontology as the basis for knowledge representation. It can express knowledge in the cyber security domain in a structural and relational way, and visualize the knowledge in a graphical manner. Security managers can use knowledge graph to intuitively understand the security intelligence, the network situation, the relationships between entities, and then discover the attributes of security-related entities, which will lay an important
foundation for understanding cyber security knowledge, analyzing cyber security data, and discovering attack patterns and abnormal characteristics related to cyber-attack.

In this paper, we summarize the application of knowledge graph in cyber security assessment. The structure is organized as follows: Section 2 presents the common cyber security assessment models and their shortcomings. Section 3 discuss the research progress of ontology-based knowledge representation and the concept of knowledge graph. Section 4 summarizes the application progress of knowledge graphs in the cyber security domain. Section 5 presents the directions of future research. Finally, we conclude the paper in section 6.

2. Common Cyber Security Assessment Models

Common cyber security assessment models include attack graph model, attack tree model, game theory model, petri net model, etc.

2.1. Concept and process of cyber security assessment

Cyber security assessment refers to the process of comprehensively analyzing and evaluating the security attributes of the information system, such as the availability, integrity, and confidentiality of the information, based on relevant information security technologies and management standards[3].

Figure 1. The process of cyber security assessment

The process of cyber security assessment mainly includes three aspects, as shown in Fig.1. First, identify the assets in the network environment, and assign value to the asset's requirements for confidentiality, integrity, and availability. Second, identify the vulnerabilities in the network environment. Third, calculate the security risk of the network environment based on the probability of the vulnerability and the impact on the confidentiality, integrity, and availability of the asset after the vulnerability is exploited.

2.2. Common Cyber Security Assessment Models

The concept of attack graph was first proposed by Philips and Swiler[1], and its purpose was to perform vulnerability analysis on the network. With the development of offensive and defensive technologies and practical needs, state attack graphs[4, 5], Bayesian attack graphs[6], and attribute attack graphs[7] have been gradually developed. Researchers also proposed attack graph generation methods based on relational and non-relational databases[8-11]. However, the attack graph is not suitable for modeling and analyzing concurrent and collaborative attack processes, and the state explosion problem is prone to occur during the generation of the attack graph, which makes the scale of the attack graph too large.

The attack tree model was first proposed by Schneier[2] to model system security threats. The model of the attack tree is relatively simple. Researchers extend the attack tree model through different methods, such as the fault tree structure integrated with attacks[12], the defensive tree model integrated with defense mechanism and game theory to solve the problem that finding the most cost-effective countermeasure set[13], the attacker-manager game tree model considering the attacker's cost per attack step[14], etc. Attack tree models are usually built for certain vulnerabilities or services, and lack a global consideration.

Game theory is widely used in the cyber security domain. Researchers establish an offensive and defensive game model by analysing the interaction between attackers and defenders, then calculate their Nash equilibrium points, and then conduct security assessment and analysis. The main models
include an offensive and defensive stochastic game model to solve the problem of defense strategy selection[15], a fully-informed dynamic game active defense model based on non-cooperative and non-zero-sum dynamic game theory[16], and a game model based on incomplete information[17-20], Markov's offensive and defensive differential game model[21], etc. Traditional game theory-based security assessment methods cannot effectively deal with the fuzzy factors in the assessment, which affects the accuracy and validity of the analysis results.

The concept of Petri net was first proposed by Carl Adam Petri in 1960, and its purpose was to describe parallel computer systems using causality. Some researchers have applied Petri nets and their improved forms to cyber security assessment and analysis. Considering different application requirements, researchers have extended classic Petri net models, such as stochastic Petri nets[22], colored Petri nets[23] and time Petri nets[24] and so on.

Researchers have also proposed network epidemic disease models[25], finite state machine models[26], and so on. Relevant research results on cyber security assessment and analysis are significant, but existing models and methods still have limitations in terms of knowledge representation and utilization. On the one hand, it is the lack of model expression capabilities. For combined cyber-attacks, most existing models lack the ability to describe concurrency and collaborative attack processes. On the other hand, the existing methods are not suitable for modeling and reasoning about empirical knowledge. During the assessment, it is necessary to evaluate the security risks faced by the system based on certain expert experience and historical data, but most model-based methods lack the ability to model and reason about empirical knowledge. Table 1 briefly summarizes the advantages and disadvantages of each model.

| Model         | Advantages                                                                 | Disadvantages                                                                 |
|---------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Attack Graph  | a) Intuitively show various possible attack paths;                         | a) State space explosion                                                       |
|               | b) Reflecting the relation-ship between system vulnerability.               | b) Not suitable for modelling and analysing con-current and collaborative attacks. |
| Attack Tree   | a) Intuitively indicate and assist the analysis of the risk of the system; | a) State space explode;                                                       |
|               | b) Easy to understand.                                                     | b) Difficult to describe large, complex, and dynamic network defense systems flexibly and effectively. |
| Game Theory   | a) Analyse network security from two aspects of attack and defense;        | a) Cannot effectively deal with the fuzzy factors in the assessment.           |
|               | b) Reason about the balanced strategy of attack and defense.               | b) Affect the accuracy and validity of the analysis results.                   |
| Petri Net     | a) Has intuitive graphical representation.                                  | a) State explosion problem                                                     |
|               | b) Mathematical foundation is strict.                                      | b) Difficult to describe a system that does not meet the characteristics of the Petri Net. |

3. Cyber security Ontology and Knowledge Graph

Ontology is used to describe concepts and relationships between concepts in a certain field or even a wider range. These concepts and relationships have a common, clear and unique definition that everyone agrees on in the shared range, which makes humans and machines can communicate with each other[27]. The ontology-based knowledge representation method can effectively combine multi-source data in a specific domain, and at the same time, the use of rich ontology language can realize the reasoning and classification of knowledge[28].

3.1. Research on Cyber security Ontology

The cyber security ontology is developed to integrate various cyber security data resources. The purpose is to organize and utilize the cyber security domain knowledge in an efficient way, and to
provide support for cyber security assessment and analysis. The research of the knowledge base based on a single ontology are rich, the most mature of which is the vulnerability description framework[29], which directly promotes the development of vulnerability databases, such as National Vulnerability Database(NVD)[30], China National Vulnerability Database of Information Security(CNNVD)[31], etc. Due to the indispensability of vulnerabilities to cyber-attacks, the research on ontology of cyber-attacks has also developed along with the research on vulnerabilities[32]. Researchers have also constructed related ontology specifically for vulnerability information management[33] and attack pattern management and exploitation[34].

For different application scenarios, researchers have developed different ontology, such as for intrusion detection[35, 36], computing node reachability matrix[37], cyber threat intelligence analysis[38], cyber security domain knowledge value assessment[39], etc. Simmonds et al.[40] built a security attack ontology model to improve people's understanding of the relationship between various elements in a cyber security system. Iannacone et al.[41] proposed a holistic ontology representing the cyber security domain, aiming to create a knowledge representation that promotes the integration of data from various structured and unstructured sources. Shed et al.[42] proposed a Unified Cybersecurity Ontology(UCO) designed to support information integration and cyber situational awareness in cyber security systems, integrating heterogeneous data and knowledge models from different network security systems, and the most commonly used network security standard for information sharing and exchange.

3.2. Knowledge Graph Overview

Ontology has a wide range of application, including but not limited to software engineering, intelligent question answering, bioinformatics, Web services (i.e., semantic Web services), retrieval systems and recommendation systems, cultural heritage protection, image understanding, and other fields. Ontology is the core of knowledge management in the knowledge graph, and its research results provide a theoretical basis for knowledge graphs to regulate entities, relationships, and the relationships between objects such as types and attributes[43].

Google introduced the concept of knowledge graph in 2012 to enhance the capabilities of its search engine. The knowledge graph is essentially a knowledge base called the semantic network[44], that is, a knowledge base with a directed graph structure. The nodes in the graph represent entities or concepts, and the directed edges represent the relationships between entities or concepts. The current knowledge graph has been used to refer to various large-scale knowledge bases. Triples are a common representation of knowledge graphs. The knowledge graph can be expressed as G = (E, R, S), where E is the set of entities in the knowledge base, R is the set of relations, S is the set of triples in the knowledge base, and the basic form of the triples includes <Entity, Relationship, Entity> and <Concept, Attribute, Attribute value>, etc. Entity is the most basic element in the knowledge graph, and different entities have different relationships. Concepts mainly refer to collections, categories, object types, types of things, such as hosts, vulnerabilities, etc. Attributes refer to the characteristics, parameters, etc. that an object may have, such as IP address, etc. Attribute values refer to the value of a specified attribute of an object, such as 192.168.1.100. Fig.2 shows an example of a simple knowledge graph. Knowledge graphs have been widely used in semantic search, knowledge answering, and knowledge-based big data analysis and decision-making[45].
The knowledge graph can be divided into general knowledge graph and industry knowledge graph. The general knowledge graph pays attention to breadth and emphasizes the integration of more entities. It is mainly used in intelligent search and other fields. The industry knowledge graph usually needs to be built on the data of a specific industry, and has specific industry significance. In the industry knowledge graph, the attributes and data models of entities are often rich and professional.

4. Application of Knowledge Graph in Cyber Security Assessment

4.1. Construction of Cyber Security Knowledge Graph

There are mature frameworks for reference to construct the knowledge graph. Both top-down construction methods [46] and bottom-up construction methods [43] can be used to build large-scale knowledge bases.

There are various mature structured knowledge bases in the cyber security domain, for example, NVD, CAPEC, etc. Jia et al. [47] used a top-down approach to propose a framework for building a cyber security knowledge graph, in which five-tuple model of security knowledge base (concepts, instances, relationships, attributes, and rules) and cybersecurity ontology (assets, vulnerabilities, and attacks) were included. However, the article only implements the construction of cyber security ontology and entity extraction, defines the rules of relationship and attribute deduction. This paper does not show the construction process of a complete cyber security knowledge graph. The cyber security ontology constructed in this paper focuses on reflecting the basic state of network assets and cannot reflect the complex situational changes in the network.

Qin [48] used a bottom-up approach to build a knowledge graph, focusing on the identification of cyber security entities and the extraction of relationships between entities in massive cyber security text data. Aiming at the shortcomings in the existing entity extraction, the author proposed a cyber security entity extraction method based on a neural network model CNN-BiLSTM-CRF combined with a feature template, and a remote supervision relationship extraction method based on ResPCNN-ATT. The focus of the research in this paper is on the theory and method of constructing a cyber security knowledge graph, and no actual application scenarios are given.

4.2. Cyber Security Situation Awareness

Utilizing the ability of knowledge graphs to integrate multi-source heterogeneous data, researchers have developed situational awareness systems for different application scenarios. In response to the problem that the existing security analysis tools only have a single data source and rely on manual analysis, researchers have developed the Stucco [49] platform to collect multi-source data and organize these data into a knowledge graph of domain concepts so that analysts and systems can quickly find related information.

CyGraph [50] is a situation awareness system developed by MITRE, which is mainly oriented towards network warfare task analysis, visual analysis and knowledge management. CyGraph aggregates isolated data and events together, and builds a knowledge graph in the cyber security domain through a unified graphic-based cyber security model. The CyGraph can analyze attack paths, predicts critical vulnerabilities, analyze intrusion alarm correlation, and interactive visual queries.

Metron [51] is a knowledge graph project developed by Apache on the basis of Cisco's OpenSOC. It integrates various open source big data technologies and can integrate the latest threat intelligence information for security monitoring and analysis.

YHSAS [52] is a situation awareness system for backbone cyber security and large-scale network environments such as large network operators, large enterprises and institutions. This system applies knowledge graphs to large-scale cyber security knowledge representation and management, enabling obtain, understand, display, and predict future development trends of the security elements that cause the network situation to change.

4.3. Cyber Security Assessment and Analysis

Aiming at the problem that existing attack graph generation and analysis methods cannot accurately reflect the true risk of nodes and attack paths, Ye et al. [53] designed a knowledge graph based on the
atomic attack ontology, and proposed an extended attack graph generation framework based on knowledge graph. Based on the framework, an attack graph generation algorithm and an attack success rate and attack profit calculation method are proposed. However, the calculation method of attack success rate and attack profit in this paper is relatively simple, and it only verifies the feasibility of the method, and does not give the application effect of the method in large-scale networks.

In consideration of unknown attacks and internal attacks, Wang et al.[54] proposed an intelligent and efficient optimal penetration path generation method to further improve the optimal penetration path generation efficiency. This method generates host threat penetration graph with the intelligent and efficient reasoning of knowledge graph, and then generate a network threat penetration graph based on penetration information exchange to obtain the optimal penetration path between any two hosts. The number of experimental network nodes in this paper is limited, which cannot reflect the advantages of knowledge graph in big data processing.

4.4. Association Analysis Based on Knowledge Graph

The Internet contains a lot of content related to cyber security, such as security blogs, hacker forums, security bulletins, intrusion alerts, and so on. Making full use of cyber security related information from various knowledge bases and websites, and associating all these security related knowledges in accordance with certain rules, will be of great significance to cyber security assessment and analysis.

Qi et al.[55] considered that the cyber-attacks have multiple attack steps, which are associated with alerts from intrusion detection systems. Based on this idea, an association analysis algorithm based on knowledge graph of cyber security attack events is proposed to show the attack scenario of air-ground integrated network. The knowledge graph is used in association analysis to display scenarios of cyber-attacks graphically.

Zhu et al.[56] proposed a cyber-attacks attribution framework based on the constructed cyber security knowledge graph to track the attack source in the air-ground integrated information network and solve the problem that the attack source is difficult to find.

There is a problem that traditional intrusion detection systems could not effectively coordinate the multi-dimensional security information stored in a separate knowledge base. Wang et al.[57] proposed an integrated intelligent security event correlation analysis system to solve the problem. The system integrated the network infrastructure knowledge base, vulnerability knowledge base, cyber threat knowledge base, and intrusion alert knowledge base into the cyber security knowledge graph to support correlation analysis of security events.

Aiming at the early detection of cyber security events (such as multi-step attacks), Narayanan et al.[58] proposed an extended cyber security ontology based on UCO. They extract host and network data to construct a cyber security knowledge graph to help security analysts detecting security incidents early, using the knowledge graph's semantic rich knowledge representation and reasoning capabilities of machine learning techniques.

5. Research Outlook

At present, some achievements have been made in the application of knowledge graphs in the cyber security domain, but in general it is still in its infancy. Further research should be carried out on the construction of cyber security ontology, cyber security assessment and analysis, prediction and traceability of cyber-attacks, and intelligent decision-making based on knowledge graphs.

5.1. Construction of Cyber Security Ontology

Ontology is the core of knowledge management in knowledge graph. The construction of cyber security ontology is directly related to whether the knowledge graph can efficiently integrate and correlate multi-source heterogeneous cyber security data. For different application scenarios in the cyber security domain, researchers have constructed different ontology models, but most of the descriptions of the ontology models are vague, and there is a lack of research on inference based on ontology. In practical applications, how to construct a suitable ontology model according to the actual
needs is the first problem to be studied in the application of knowledge graphs to the cyber security domain.

5.2. Cyber Security Assessment and Analysis

Existing cyber security assessment and analysis methods are mostly based on attack graphs, the methods are relatively simple, and they are limited by the scalability of attack graph models. We should combine existing assessment models and analysis methods (i.e., Bayesian nets) with knowledge graph technology to make full use of the advantages of knowledge graph in relational data processing, data fusion and knowledge reasoning, and then improve the efficiency of cyber security assessment. This will be the direction of further research.

5.3. Prediction and traceability of cyber attacks

The existing research on association analysis can only perform association analysis on simple cyber-attacks or events, and lacks research on the prediction and traceability of complex cyber-attacks. For security events that occur in the network, how to correlate the events to network assets, obtain the context information of the events, and then predict and trace the events are the key and difficult issues in the cyber security domain.

5.4. Intelligent decision-making based on knowledge graph

In cyber security assessment, how to implement intelligent decision-making based on cyber situation is the development trend of cyber security assessment. The current cyber security assessment also relies on personal experience, and the level of intelligence is low. Improving the intelligence level of cyber security assessment is a problem that needs to be solved urgently. Wei et al. [59] proposed an intelligent decision-making model based on knowledge graph to solve the shortcomings of traditional decision-making models in terms of flexibility, knowledge representation and collaboration. Based on the knowledge graph technology, it is worthwhile to study the decision model applicable to cyber security and improve the intelligence level of cyber security assessment.

6. Conclusions

In this paper, we discuss the application of knowledge graphs in cyber security assessment, introduce common cyber security assessment models and methods, and points out their shortcomings. Then, we introduce the research progress of ontology-based knowledge representation in the cyber security domain and the concept of knowledge graph, analyze the advantages of applying knowledge graph to cyber security assessment; then expound the related research situation of knowledge graph in cyber security assessment. Finally, based on the shortcomings of existing research, the future research directions are prospected.

Knowledge graphs have been widely used in intelligent search, intelligent question answering, personalized recommendation, intelligence analysis, anti-fraud and other fields. Applying knowledge graphs to the cyber security domain will be the forefront research direction in this field.

References
[1] C. Phillips, L. Swiler, A graph-based system for network-vulnerability analysis, ACM, 1998, 71-79.
[2] B. Schneier, Attack trees: modeling security threats, Dr Dobb’s Journal, 24(1999),21-29.
[3] X. Gao. Research on the Theories and Key Technologies of Network Security Assessment. PLA Information Engineering University, Zhengzhou, 2014.
[4] S. Jha, O. Sheyner, J. Wing, Two formal analyses of attack graphs, IEEE, 2002, 49-63.
[5] O. Sheyner, J. Haines, S. Jha, et al, Automated generation and analysis of attack graphs, 2002.
[6] Y. Liu, H. Man, Network Vulnerability Assessment Using Bayesian Networks, Proceedings of SPIE - The International Society for Optical Engineering, (2005).
[7] L. Wang, Y. Chao, A. Singhal, et al, Interactive Analysis of Attack Graphs Using Relational Queries, Lecture Notes in Computer Science, 4127(2008),119-132.
[8] M. S. Barik, C. Mazumdar, A. Gupta, Network Vulnerability Analysis Using a Constrained Graph Data Model, 2016.
[9] M. S. Barik, C. Mazumdar, A Graph Data Model for Attack Graph Generation and Analysis, 2014.
[10] S. Noel, E. Harley, K. H. Tam, et al, Big-Data Architecture for Cyber Attack Graphs, (2014).
[11] L. Wang, Y. Chao, A. Singhal, et al, Implementing interactive analysis of attack graphs using relational databases, Journal of Computer Security, 16(2008),419-437.
[12] I. N. Fovino, M. Masera, A. D. Cian, Integrating cyber attacks within fault trees, Reliability Engineering & System Safety, 94(2009),1394-1402.
[13] S. Bistarelli, M. Dall Aglio, P. Peretti, Strategic Games on Defense Trees., 2006.
[14] A. Arghavani, M. Arghavan, M. Ahmadi, et al, Attacker-Manager Game Tree (AMGT): A New Framework for Visualizing and Analysing the Interactions Between Attacker and Network Security Manager, Computer Networks, 133(2018).

[15] W. Jiang, B. X. Fang, Z. H. Tian, et al. Research on Defense Strategies Selection Based on Attack-Defense Stochastic Game Model. Journal of Computer Research and Development. 47(2010), 1714-1723.
[16] W. Q. Lin, H. Wang, J. H. Liu, et al. Research on Active Defense Technology in Network Security Based on Non- Cooperative Dynamic Game Theory. Journal of Computer Research and Development. 48(2011), 306-316.
[17] Q. K. Mi, B. Wu, Y. Du, et al. Information System Security Risk Assessment Based on Incomplete Information Security. JISUANJI YU XIANDAIHUA. (2019), 118-126.
[18] H. Q. Zhang, J. N. Yang, C. F. Zhang. Defense decision-making method based on incomplete information stochastic game and Q-learning. Journal on Communications. 39(2018), 56-68.
[19] J. N. Yang, H. Q. Zhang, C. F. Zhang. Defense decision-making method based on incomplete information stochastic game. Chinese Journal of Network and Information Security. 4(2018), 12-20.

[20] J. D. Wang, D. K. Yu, H. W. Zhang, et al. Defense Strategies Selection Based on Incomplete Information Attack-Defense Game. Journal of Chinese Computer Systems. 36(2015), 2345-2348.
[21] H. Zhang, S. Huang. Markov Differential Game Model and Its Application in Network Security. ACTA ELECTRONICA SINICA. 47(2019), 606-612.
[22] N. H. Yang, H. Q. Yu, Z. L. Qian, et al, Modeling and quantitatively predicting software security based on stochastic Petri nets, Mathematical & Computer Modelling, 55(2012),102-112.

[23] R. Laborde, B. Nasser, F. Grasset, et al, A Formal Approach for the Evaluation of Network Security Mechanisms Based on RBAC Policies, Electronic Notes in Theoretical Computer Science, 121(2005),117-142.
[24] S. Pudar, G. Manimaran, C. C. Liu, PENET: A practical method and tool for integrated modeling of security attacks and countermeasures, Computers & Security, 28(2009),754-771.
[25] C. Vargas-De-León, On the global stability of SIS, SIR and SIRS epidemic models with standard incidence, Chaos Solitons & Fractals, 44(2011),1106-1110.
[26] W. Guo, J. Wu, F. Zhang, et al. A Cyberspace Attack and Defense Model with Security Performance Analysis Based on Automata Theory. Journal of Cyber Security. (2016), 29-39.
[27] X. Y. Du, M. Li, S. Wang. A Survey on Ontology Learning Research. Journal of Software. 17(2006), 1837-1847.
[28] J. B. Gao. Research on Ontology Model and Its Application in Information Security Evaluation. Shanghai Jiao Tong University, 2015.
[29] R. C. Seacord, A. D. Householder, A Structured Approach to Classifying Security Vulnerabilities, (2005).
[30] Information on https://nvd.nist.gov/.
[31] Information on http://www.cnvd.org.cn/.
[32] R. Syed, H. Zhong, Cybersecurity Vulnerability Management: An Ontology-Based Conceptual Model, New Orleans, United States, 2018.
[33] Y. Zhu, Attack Pattern Ontology: A Common Language for Cyber Security Information Sharing, (2015).
[34] A. Joshi, R. Lal, T. Finin, et al, Extracting Cybersecurity Related Linked Data from Text, 2013.
[35] V. Mulwad, W. Li, A. Joshi, et al, Extracting Information about Security Vulnerabilities from Web Text, 2011.
[36] J. Undercoffer, A. Joshi, J. Pinkston, Modeling Computer Attacks: An Ontology for Intrusion Detection, 2003.
[37] N. Scarpato, N. D. Cilia, M. Romano, Reachability Matrix Ontology: A Cybersecurity Ontology, Applied Artificial Intelligence, (2019),1-13.
[38] C. Lederer, S. Altstadt, S. Andriamonje, et al, An ontology for threat intelligence, Munich, Germany, 2016.
[39] A. Aviad, K. Węcel, W. Abramowicz, A Concept for Ontology-Based Value of Cybersecurity Knowledge, International Journal of Management and Economics, (2018).
[40] A. J. Simmonds, P. Sandilands, L. V. Ekert, An Ontology for Network Security Attacks, 2004.
[41] M. Iannacone, S. Bohn, G. Nakamura, et al, Developing an Ontology for Cyber Security Knowledge Graphs, 2015.
[42] Z. Syed, A. Padia, T. Finin, et al, UCO: A Unified Cybersecurity Ontology, 2016.
[43] Q. Liu, Y. Li, H. Duan, et al. Knowledge Graph Construction Techniques. Journal of Computer Research and Development. 53(2016), 582-600.
[44] G. L. Qi, D. T. Ouyang, J. Z. Li. Ontology Engineering and Knowledge Graph Topic Introduction. Journal of Software. 29(2018), 5-6.
[45] J. Li, L. Hou. Reviews on Knowledge Graph Research. 40(2017), 454-459.
[46] Y. J. Yang, B. Xu, J. W. Hu, et al. Accurate and Efficient Method for Constructing Domain Knowledge Graph. Journal of Software. 29(2018), 39-55.
[47] Y. Jia, Y. Qi, H. J. Shang, et al. A Practical Approach to Constructing a Knowledge Graph for Cybersecurity. Engineering. v.4(2018), 117-133.
[48] Y. Win. Research on Key Technologies of Network Security Knowledge Graph Construction. Guizhou University, Guizhou, 2019.
[49] Information on https://stucco.github.io/.
[50] S. Noel, E. Harley, K. H. Tam, et al, CyGraph: Graph-Based Analytics and Visualization for Cybersecurity, Handbook of Statistics, (2016).
[51] Metron, http://metron.apache.org/.
[52] Y. Jia, W. H. Han, W. Wang. Research and Implementation Security Situation Analysis and Prediction System for Large-scale Network. INFORMATION TECHNOLOGY AND NETWORK SECURITY. 37(2018), 17-22.
[53] Z. W. Ye, Y. B. Guo, T. Li, et al. Extended Attack Graph Generation Method Based on Knowledge Graph. Computer Science. (2019), 1-14.
[54] S. Wang, J. H. Wang, G. M. Tang, et al. Intelligent and Efficient Method for Optimal Penetration Path Generation. Journal of Computer Research and Development. 56(2019), 929-941.
[55] Q. Y., J. R., J. Y., et al, Association Analysis Algorithm Based on Knowledge Graph for SPACE-Ground Integrated Network, 2018, 222-226.
[56] Z. Z., J. R., J. Y., et al, Cyber Security Knowledge Graph Based Cyber Attack Attribution Framework for Space-ground Integration Information Network, 2018, 870-874.
[57] W. Wei, J. Rong, J. Yan, et al, KGBIAC: Knowledge Graph Based Intelligent Alert Correlation Framework, 2017.
[58] S. Narayanan, A. Ganesan, K. Joshi, et al, Cognitive Techniques for Early Detection of Cybersecurity Events, 2018.
[59] J. Wei, W. H. Li, W. Pan. Research on Intelligent Decision Support Technology and Application Based on Knowledge Graph. COMPUTER TECHNOLOGY AND DEVELOPMENT. (2020), 1-6.