Eng Int Syst (2021) 6: 379–386
© 2021 CRL Publishing Ltd

Engineering
Intelligent Systems

Research on Network Security Collaborative Defense Technology Based on Swarm Intelligence and Big Data Network Security

Yu Bingjie*, **Yang Huifeng, Sun Chenjun, Zhang Zhi and Fan Jinghang**

State Grid Hebei Information & Telecommunication Branch; Shijiazhuang, Hebei 050000, China

Currently, Internet technology and the construction of Internet platforms are undergoing a great deal of development with new technologies being applied to upgrade and optimize the performance of various Internet platforms, which in turn creates a good environment for the development of various network technologies. The evolution of technology for cloud computing and the Internet of Things (IoT), has led to changes in data types and data processing methods. Moreover, the network technologies have generated a great deal of unstructured data, greatly enriching the content of network databases and ushering in the era of big data. The rich resources offered by the big data platform and their potential for resolving problems and improving efficiency, can be used to advantage but only if big data and data fusion processes are well-understood. Much of the research and analysis of the technologies related to big data have been inspired by patterns of behaviour observed in insect communities, which has led to the development and optimization of the swarm intelligence algorithm. This paper examines and analyzes the security issues associated with the Internet platform, proposes a collaborative network security defense mechanism, and provides a reference for the construction of a secure Internet environment.

Keywords: swarm intelligence; big data; network security; collaborative defense

1. INTRODUCTION

Internet technology and the construction of Internet platforms have undergone a great deal of development, with continuous upgrade and optimization, facilitating the further development of various network technologies. This has led to the evolution of cloud computing technology and the Internet of Things, and changes to data types and data processing methods [1]. New network technologies have enriched the content of network databases, generated a great amount of unstructured data, and ushered in the era of big data that offers new directions and opportunities for the development of various network technologies. More types of data information have appeared in the network system and various industries have begun to integrate big data technology. For many companies, this has become a major driving force of their development, enabling the dissemination of information and the efficient processing of data [2]. Moreover, data resources have become more secure, and people can obtain all kinds of resources very quickly which is advantageous for those who require prompt solutions to complex problems. Big data technology can provide communication between resources, and can analyse visual data, which reflects the main content of group wisdom to a certain extent. Long-term research and experience have led researchers to observe the natural habits of social animals, and have applied their knowledge to the development of big data technology [3]. Analysis has shown a degree of similarity between human problem solving and the exchange of resources by social animals. This has provided insights for

*Address for correspondence: Yu Bingjie, State Grid Hebei Information & Telecommunication Branch; Shijiazhuang, Hebei 050000, China, Email: ybj20201210@126.com the development of problem-solving strategies for big data. Inspired by the living habits of social animals, the researchers proposed a swarm intelligence optimization algorithm [4]. This algorithm can combine resources in various fields to analyze data and to improve the flexibility and scientific of mathematical models; thus, the intelligent optimization algorithm offers development opportunities to many industries.

Since the advantages of this algorithm can be exploited to solve several very complex problems, many researchers apply it to unpredictable key designs. This algorithm can also be used to inspect the security of network system operations, and perform cluster analysis of the data sources of the intrusion network system [5]. Therefore, the algorithm is also the main technical support used to maintain the safe operation of the network system, providing a strong mechanism for security defense. In this era of big data, it has been found that the most likely problem faced by data transmission and information exchange in cyberspace is security. Hence, the protection of network security is crucial for big data, making it necessary to conduct research on group intelligence algorithms. This paper examines and analyzes the security issues associated with the Internet platform, and proposes a collaborative network security defense mechanism which can be the basis for the construction of a secure Internet environment [6]. To carry out this work, the researchers applied the concept of layering and segmentation, and established corresponding security control systems for the inner and outer layers of the Internet space. The establishment of a network security mechanism is related to the security of the entire Internet system. Therefore, researchers and Internet platform managers need to adopt appropriate methods to utilize network monitoring resources and combine various network security technologies to improve the overall security of the Internet platform. In view of current technological developments, the aim of this study is to examine and analyze two different Internet security mechanisms: the collaborative monitoring mechanism and the collaborative linkage mechanism [7]. The collaborative monitoring mechanism uses resource coordination technology, which can help monitor the operation of multiple monitoring devices in the network. The main function of the second monitoring mechanism is to strengthen the firewall construction of the Internet security system, link the security monitoring equipment with improved firewall functions, and use SNMPv3 to establish communication links. In this study, the analyzed security mechanism was tested by establishing a mathematical model, programming and programming were used to simulate actual network environment operations, and conclusions were drawn from the analysis of experimental results.

2. ANALYSIS OF CROWD INTELLIGENCE ALGORITHMS AND NETWORK SECURITY PRINCIPLES IN THE ERA OF BIG DATA

2.1 The Concept and Characteristics of Network Swarm Intelligence

2.1.1 Concept

Today, the Internet is an important platform for the construction of information networks. When constructing these, project personnel can organically combine experimental projects in different regions to achieve the work of each pilot, and can communicate with each other remotely in real time, learn from each other's successes and become aware of emerging problems [8]. This can effectively prevent the recurrence of problems during the construction of the pilot project, greatly improving its public value. In this era of Internet development, the users have gradually obtained more control of network information and ensuring user satisfaction with the services provided by Internet platforms has become the main aim of Internet development. Hence, the users have become the focus of Internet platform development, given the great amount of information that is constantly being conveyed, exchanged and disseminated [9]. To cater for users' needs, the clustering analysis of network data has been greatly improved, and the development of intelligent information interaction in the era of big data has gradually become the means of solving problems. Nowadays, each individual can be integrated into the construction of the Internet network, which results in a huge intelligent decision-making network, which is also a realistic embodiment of group wisdom.

The big data era has seen the communication between people become closer. People today have more channels for communication, information exchange and the sharing of resources, all of which have become more frequent and characteristic of communication networks. A huge group communication network is also a concrete manifestation of group behavior [10]. Group behavior will be manifested through a variety of different modes, and the level of group intelligence will also change to a certain extent according to the level of people's communication. People's group behavior in the context of big data is, in a sense, the manifestation of network group intelligence. Users can search the network for strategies and resources to solve problems, which can strengthen interpersonal communication. Big data technology enables users' data information to be effectively stored. When problem-solving, researchers can determine the user's specific situation by analyzing the user's behavior on the Internet platform, and evaluating the user's main behavior within the group.

2.1.2 Features

The main support for the development of the big data era is the continuous improvement of the intelligence level of the network group. The group intelligence of a network can provide a variety of problem-solving strategies and models for the development of the big data network since it offers sharper thinking, more flexible information retrieval, and knowledge [11]. The system is relatively complete, the emotional association is rapid, and it contains rich experience and a wealth of commonsense. Unlike Turing machine intelligence and traditional swarm intelligence, network swarm intelligence can comprehensively utilize various resources to find solutions to problems, although these two development models also have their own advantages. Turing machine intelligence has a powerful data operation function, and can provide extremely strong logic analysis ability for data retrieval and information analysis. However, it is possible to combine Turing machine intelligence with network swarm intelligence, give full play to the advantages of both, and improve the ability of swarm intelligence to solve and analyze problems.

2.2 Application Principle of Swarm Intelligence Algorithm

Researchers have designed a swarm intelligence algorithm by observing the natural habits of social animals. The application of this algorithm can effectively simulate and analyze the group behavior of a variety of social animals in nature [12]. Communities of social animals will find food according to an instinctive method of cooperation. Each animal in the group learns the predation experience of other animals, and they will master the main directions and methods of finding food targets. The behavior of gregarious animals looking for food is one where each individual obtains benefits from the group's mutual learning and interaction, which is the advantage of group intelligence. The main principle underlying the swarm intelligence algorithm is the process of determining the location of food being sought by gregarious animals [13]. This kind of algorithm can be used to deal with complex problems and achieve optimal solutions. It can judge the appropriateness of the chosen solution through specific calculations. The optimal solution can be calculated with:

$$X_i = (x_1, x_2, L, x_n)(1, 2, L, n) \tag{1}$$

$$\min f(x)$$
$$s.t. g_j(X) \leq 0,\ j = 1, 2, L, m, \tag{2}$$
$$X \in \Omega$$

2.3 Network Information Security Control Mechanism Model in The Context of Big Data

2.3.1 Staff Layer-Core Motivation

During the operation of the network platform, the source of information and the way it is obtained by users is the main reason for security problems associated with network information. To ensure that the interests of users are not compromised, a secure network protection mechanism must be established. For this task, the personnel responsible for maintaining the network system are the main people in control of operating the security mechanism and ensuring network security [14]. The management layer of the security system has several components: the users of the network platform, the managers of the network operation, the businesses that provide various types of network information, and the saboteurs and attackers who pose threats to the network system. Users of network platforms should improve their ability to review information, take the initiative to prevent the dissemination of false information, and contribute to the creation of a safe and harmonious network environment.

2.3.2 Environmental Layer-Environmental Support

The environmental layer must be considered when establishing a security mechanism as it is essential for the operation of this mechanism, as it facilitates the safe operation of the network environment and ensures the normal use of network facilities [15]. With the development of a social economy, various technologies are being applied in industry and in people's everyday activities. The development of information technology and network technology has given people a broader platform for information dissemination and communication, and the processing of data on a global scale. The continuous improvement of database management, the ongoing development of information technology, and the construction of various types of information systems have increasingly assisted and improved the operations of various industries. However, these technological advancements have placed pressure on the carrying capacity of the Internet platform [16]. The large amount of data generated by network operations and and the methods applied to data analysis will give the big data platform calculations. The system has an impact. In the era of big data, improving the ability of network systems to store and analyze data is the main reason for ensuring the safe operation of network systems [17].

3. DESIGN AND IMPLEMENTATION OF COLLABORATIVE NETWORK SECURITY DEFENSE MECHANISM

3.1 System Overall Design and Implementation Method

The security defense system and the operation mode designed in this paper are depicted in Figure 1 below.

3.2 Mathematical Principles of Collaborative Technology

In the analysis process, it is assumed that there is one management center and multiple monitoring centers in all monitoring equipment. In order to test the performance of the resource collaborative monitoring equipment in reality, it is necessary to evaluate and analyze the monitoring efficiency of the equipment and the efficient utilization of resources. Through analysis and derivation, we obtain:

$$\sum_{i=1}^{n} N_{i,j,z} = N_{i,j,z} = (0, 1) \tag{3}$$

If the monitoring resources of each device are the same, then the monitoring efficiency of each device for a specific period of time is:

$$N_i = \frac{1}{m} \sum_{j=1}^{m} \sum_{i=1}^{n} N_{i,j,z} \tag{4}$$

If the resources of the monitoring center are totally consumed within a certain period of time, the monitoring objects in the task list may be actively abandoned by the system. Assuming that a monitoring object is discarded, we obtain:

$$\sum_{i=1}^{n} N_{i,m,j} = N_{i,m,j} = 0 \tag{5}$$

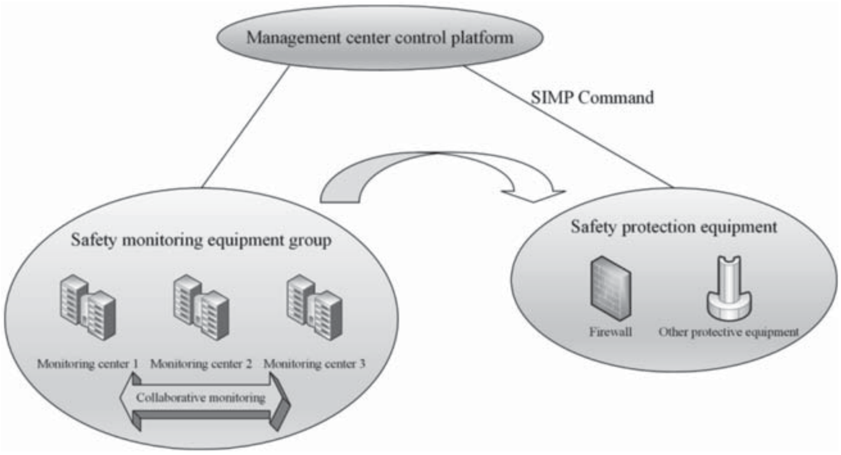
Management center control platform
SIMP Command
Safety monitoring equipment group
Monitoring center 1
Monitoring center 2
Monitoring center 3
Collaborative monitoring
Safety protection equipment
Firewall
Other protective equipment

Figure 1 Method for realization of coordinated defense mechanism.

$$
\begin{aligned}
\bar{U}_{t+dt} &= \frac{\sum_{i=1,i\neq y}^{n-1} U_{i,t+dt} + U_{m,t+dt} + U_{y,t+dt}}{n} \\
&= \frac{\sum_{i=1,i\neq y}^{n-1} U_{i,i} + \sum_{j=1}^{n} U_{y,j,t+dt} \bullet N_{y,j,t+dt} + \sum_{j=1}^{m} U_{n,j,t+\Delta t} \bullet N_{n,j,t+\Delta t}}{n} \\
&= \frac{\sum_{i=1,i\neq y}^{n-1} U_{i,t} + U_{y,m,t} + \sum_{j=1}^{m-1} U_{y,j,i} \bullet N_{y,j,i} + \sum_{j=1}^{m-1} U_{n,j,z} \bullet N_{n,j,z}}{n} \\
&= \frac{\sum_{i=1}^{n} U_{i,t} + U_{i,t} + U_{y,m,t}}{n} = \bar{U}_t + \frac{U_{y,m,t}}{n} > \bar{U}_t
\end{aligned} \tag{12}
$$

Through deformation, this is obtained:

$$N_i = \frac{1}{m}\sum_{j=1}^{m-1}\sum_{i=1}^{n} N_{i,j,z} \tag{6}$$

The resource usage of monitoring equipment in another time period can be obtained with this calculation:

$$\sum_{i=1}^{n} N_{i,m,z+\Delta z} = N_{y,m,z+\Delta z} = 1 \tag{7}$$

The monitoring efficiency of the monitoring instrument at this time is:

$$N_{t+\Delta t} = \frac{1}{m}\sum_{j=1}^{m}\sum_{i=1}^{n} N_{i,j,t+\Delta t} = N_t + \frac{1}{m} > N_t \tag{8}$$

For a specified period of time, the consumption of resources after the monitoring center has completed all monitoring tasks can be expressed as:

$$U_{Lt} = \sum_{j=1}^{m} (U_{i,j,t} \bullet N_{i,j,t}) \tag{9}$$

Assuming that the ability of each monitoring center to complete the task is the same, then:

$$\bar{U}_t = \frac{1}{n}\sum_{i=1}^{n} U_{i,t} \tag{10}$$

There is also the need to consider resource exhaustion, which can be expressed as:

$$\overline{U}_t = \frac{1}{n}\left(\sum_{i=j}^{n-1} U_{i,t} + \sum_{j=1}^{m-1}\left(U_{n,j,t} \bullet N_{n,j,t}\right)\right) \tag{11}$$

The average resource utilization at this time can be expressed as:

3.3 Experimental Environment Construction

In this study, a small experimental environment was constructed to test the efficiency of the coordination mechanism. The experimental environment is shown in Figure 2 below.

In this study, a small experimental environment was constructed to test the effectiveness of the coordination mechanism. The experimental environment is depicted below in Figure 3.

3.4 Performance Analysis of Collaborative Network Security Defense Mechanism

In order to analyze the main performance of the security mechanism, this study was verified through experiments. The results of the experiment are shown in Table 1 below.

The data presented in Table 2 and Table 3 indicates that the increase in the number of communication hosts will reduce the efficiency of the monitoring equipment.

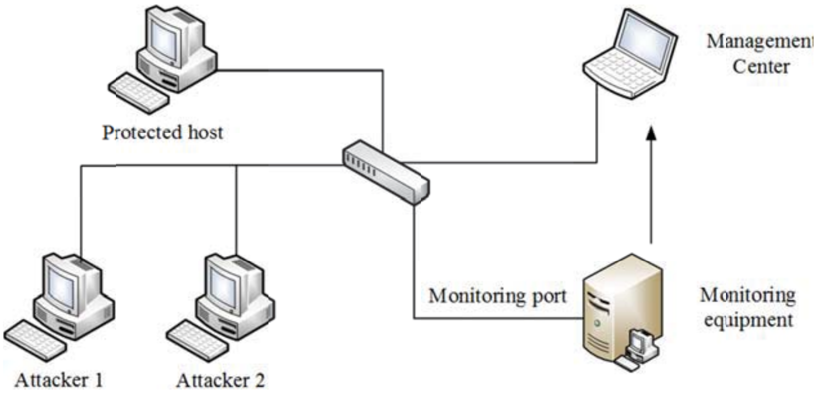

Figure 2 Lab environment.

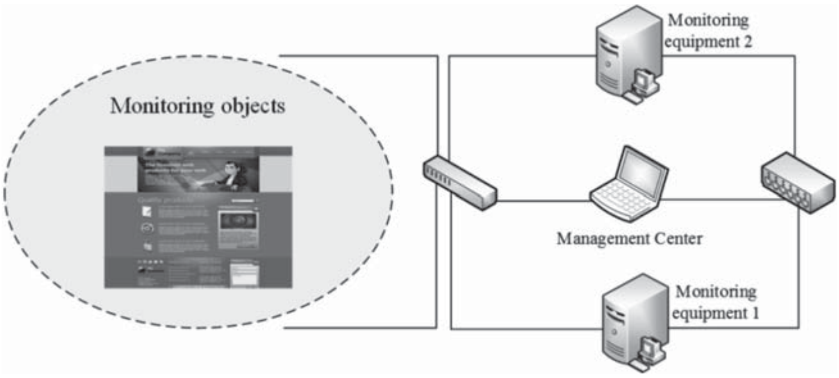

Figure 3 Lab environment.

Table 1 The work of a single monitoring center.

Number of host pairs	2	3	4	5	6	7
Number of data packets recorded C	2492	3677	4655	5377	4687	4204
Monitoring efficiency Ni	99%	98%	93%	86%	62%	48%

Table 2 Resources collaborate with the work of the first two monitoring centers.

Task Assignment	5:5	4:6	3:7	2:8	1:9	0:10
Number of data packets recorded by monitoring center 1	5391	4695	3707	2500	1255	9
Number of data packets recorded by monitoring center 2	5372	4710	5588	6099	6870	7098
Peak CPU utilization rate of monitoring center 1%	84.3	92.5	99.2	98.9	99.6	99.6
Peak CPU utilization rate of monitoring center 2%	84.9	72.0	64.9	52.0	30.9	14.7

Table 3 The work of the two monitoring centers after resource coordination.

Task Assignment	5:5	4:6	3:7	2:8	1:9	0:10
Number of data packets recorded by monitoring center 1	5654	5336	5182	5155	5153	5125
Number of data packets recorded by monitoring center 2	5600	5413	5223	5234	5222	5206
Peak CPU utilization rate of monitoring center 1%	86.3	84.3	84.7	86.2	86.4	87.7
Peak CPU utilization rate of monitoring center 2%	85.7	85.5	86.5	87.7	87.6	89.4

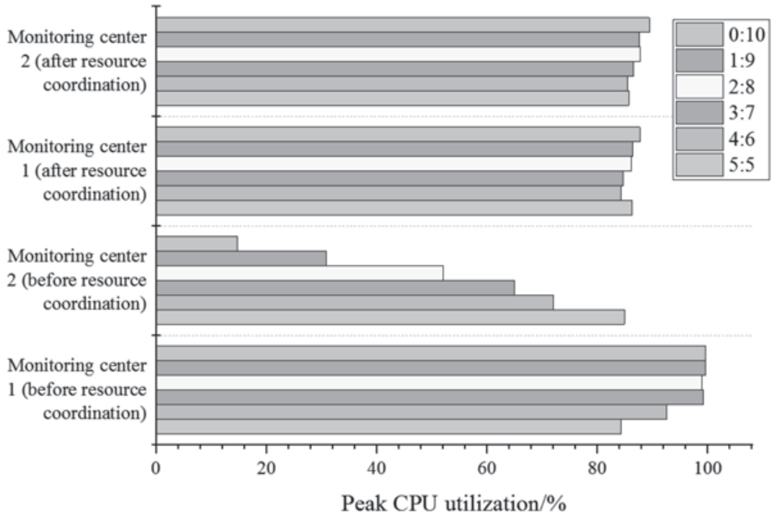

Figure 4 Comparison of the work situation of the two monitoring centers before and after resource coordination.

Table 4 Confirmatory analysis results.

Dimension	Item	Model parameter estimates				Reliability and validity			
		Non-standardized factor loading	Standard error S.E.	C.R. (t-value)	P	Normalized factor loading	SHC	CR combination reliability	Mean square deviation
The internet	Q1	1				0.716	0.513		
Control	Q2	1.084	0.128	8.476		0.804	0.646	0.798	0.569
Personnel	Q3	1.097	0.133	8.257		0.740	0.548		
	Q4	1				0.968	0.937		
Surroundings	Q5	0.761	0.066	11.617		0.662	0.438	0.915	0.787
	Q6	1.038	0.028	37.350		0.993	0.986		
	Q7	1				0.762	0.581		
Technology	Q8	1.103	0.114	8.851		0.750	0.563	0.765	0.521
	Q9	0.952	0.128	7.435		0.648	0.420		
The internet	Q13	1				0.967	0.935		
Information	Q14	0.992	0.037	27.159		0.964	0.929	0.929	0.815
Safety	Q15	0.890	0.060	14.745		0.763	0.582		
Standard		—	>0	>1.96	<0.05	>0.6	>0.36	>0.7	>0.5

4. BIG DATA NETWORK SECURITY EFFECT ANALYSIS

4.1 Evaluation Model Design

When establishing a network security mechanism, three factors will determine the effectiveness of this mechanism: the personnel controlling platform operations, the operation of the network environment, and the use of security technology [18]. This paper evaluates the effectiveness of the security mechanism by constructing a mathematical model.

4.2 Reliability and Validity Test of Questionnaire Data

This study uses confirmatory analysis methods to test the validity and reliability of the questionnaire. The results of the analysis are shown below in Table 4.

4.3 Construction of Big Data Network Security Weight System

This article uses the analytic hierarchy process to evaluate the conditions of each indicator. The results of the analysis are shown below in Table 5.

5. CONCLUSION

In the current era of development, the development of the Internet has gradually entered the stage of intelligent development, and the development of network group intelligence is the main support for the development of the Internet. In the development of the big data era, the effective processing of information and the safe operation of network platforms are the main contents of people's research. This article studies and analyzes the security issues of the Internet platform, introduces the situation of collaborative network security defense mechanisms to people, and provides a

Table 5 Weight Index System of Network Information Security Control System.

Level 1 indicator T	First-level weight	Secondary index C	Secondary weight	Level three index P	Three-level weight
Personnel T1	0.297	Network corpse C1	0.120	Network User Safety Education P1	0.106
				Network user security awareness P2	0.633
				Self-management of network corpses P3	0.261
		Network information service provider C2	0.272	Provider Security Responsibility P4	0.500
				Provider safety behavior P5	0.500
		Manager C3	0.608	Managerial technical ability P6	0.539
				Management staff job safety literacy P7	0.164
				Managerial Professionalism P8	0.297
Environment T2	0.164	Network facilities C4	0.231	Network facility carrier capacity P9	0.500
				Network facility data processing capability P10	0.500
		Network Culture C5	0.104	Network culture cultivation P11	0.750
				Network culture purification P12	0.250
		Policies and regulations C6	0.665	Network Information Security Implementation Standard P13	0.231
				Network Information Security Code of Conduct P14	0.104
				Network Information Security Legislation P15	0.665
Technology T3	0.539	Fire blocking technology C7	0.250	Network user access authority P16	0.371
				User access authentication P17	0.371
				Anti-denial of service attack P18	0.151
				Anti-malware P19	0.107
		Encryption technology C8	0.250	Storage encryption technology P20	0.500
				Communication encryption technology P21	0.500
		Security Monitoring Technology C9	0.250	Application system access control P22	0.333
				Data seat system access control P23	0.333
				Operating system access control P 24	0.333 0.080
		Security Audit Technology C10	0.250	Application system log audit P25	0.080
				Database system log audit P26	0.080
				Operating system log audit P27	0.080
				Intrusion detection control audit P28	0.262
				Antivirus upgrade audit P29	0.498

certain reference for the construction of the Internet security environment. When studying and analyzing the establishment of Internet security mechanisms, the researchers made full use of the idea of layering and segmentation, and established corresponding security control systems for the inner and outer layers of the Internet space. The establishment of a network security mechanism is necessary for the security of the entire Internet system. Therefore, researchers and Internet platform managers need to adopt appropriate methods to utilize network monitoring resources and combine different network security technologies to ensure the security of the Internet platform.

REFERENCES

1. A. Yousefpour, R. Ibrahim, Hamed HNA. Ordinal-based and frequency-based integration of feature selection methods for sentiment analysis. *Expert Syst. Appl.* 751 (2017), 80–93.
2. W. Zhang, C. Yu, W. Meng, Opinion retrieval from blogs. In: *Proceedings of the Sixteenth ACM Conference on Information and Knowledge Management* 35(4) (2007), 831–840.
3. P. Zhao, L. Hou, O. Wu. Modeling sentiment dependencies with graph convolutional networks for aspect-level sentiment classification. *Knowl. Based Syst.* 1936 (2020), 105–143.
4. Z. Zheng, X. Wu, R. Srihari. Feature selection for text categorization on imbalanced data. *ACM SIGKDD Explor. Newsl.* 6(1) (2004), 80–89.
5. A. Atzeni, F. Diaz, A. Marcelli, et al. Countering android malware: a scalable semi-supervised approach for family-signature generation. *IEEE Access* 6 (2018), 59540–59556.
6. R.J. Bagnall, G. French. The Malware Rating System (MRS)TM. In: *Proceedings of the 6th International Command and Control Research and Technology Symposium. Annapolis* 53(3) (2001), 536–542.
7. P. Bhat, K. Dutta, A survey on various threats and current state of security in android platform. *ACM Comput. Surv.* 52(1) (2019), 1–35.
8. F. Biondi, F. Dechelle, A. Legay MASSE: Modular automated syntactic signature extraction. In: *Proceedings—2017 IEEE 28th International Symposium on Software Reliability Engineering Workshops, ISSREW* 34(5) (2017), 96–97.
9. A. Damodaran, F.D. Troia, C.A. Visaggio, et al. A comparison of static, dynamic, and hybrid analysis for malware detection. *J. Comput. Virol. Hacking Tech.* 13(1) (2017), 1–12.
10. L. Davi, A. Dmitrienko, C. Liebchen, et al. Over-the-air cross-platform infection for Breaking mTAN-based online banking authentication 72(6) (2012), 45–63.
11. M. Egele, T. Scholte, E. Kirda, C. Kruegel. A survey on automated dynamic malware-analysis techniques and tools. *ACM Comput. Surv.* (CSUR) 44(2) (2012), 1–42.
12. W. Enck, P. Gilbert, S. Han, et al. TaintDroid. *ACM Trans. Comput. Syst.* 32(2) (2014), 1–29.
13. P. Faruki, A. Bharmal, V. Laxmi, et al. Android security: a survey of issues, malware penetration, and defenses. *IEEE Commun. Surv. Tutorials* 17(2) (2015), 998–1022.
14. A. Gopalakrishnan, E. Vineti, A.K. Mohan, M. Sethumadhavan. The art of piecewise hashing: a StepToward better evidence provability. *J. Cyber Security Mobility* 7(1) (2018), 109–130.
15. J. Li, L. Sun, Q. Yan, et al. Significant permission identification for machine-learning-based android malware detection. *IEEE Trans. Indu. Inform.* 14(7) (2018), 3216–3225.
16. M. Odusami, O. Abayomi-Alli, S. Misra, et al. Android malware detection: a survey. In: *Communications in Computer and Information Science*, vol. 942 (2018), 255–266.
17. M. Kumar, Y.H. Mao, Y.H. Wang, et al. Fuzzy theoretic approach to signals and systems: static systems. *Inform. Sci.* 418 (2017), 668–702.
18. W.P. Zhang, J.Z. Yang, Y.L. Fang, et al. Analytical fuzzy approach to biological data analysis. *Saudi J. Biol. Sci.* 24(3) (2017), 563–573.