Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 4, pp. 2596–2602, DOI 10.12694/scpe.v25i4.2901

VERIFICATION AND OPTIMIZATION OF NETWORK SECURITY DEFENSE SYSTEM FROM THE PERSPECTIVE OF BLUE ARMY IN ACTUAL OFFENSIVE AND DEFENSIVE EXERCISES

ZHOUYUAN LIAO[*], ZHENHONG ZHANG[†], AND YING YAN[‡]

Abstract. From the point of view of signal camouflage, this paper proposes an active network defense system. Then, the optimal camouflage target selection scheme is proposed. Its goal is to solve the problems existing in the information construction of Chinese military equipment support. This method establishes a multistage game model based on weapon support information network attack and defense. The attack and defense benefits are quantitatively calculated based on the cost of signal concealment. The solution to the refined Bayesian balance problem is given. Then, a multistage optimization algorithm for camouflage signal selection is proposed. Finally, experimental research proves the proposed algorithm to be reasonable and practical.

Key words: Actual combat offensive and defensive exercise; Information network; Multistage signal game; Optimal camouflage signal

1. Introduction.

In the attack and defense confrontation of the weapon support system, if the appropriate concealed signal can be selected and the concealed signal can be used to interfere with the attacker's behavior, the defensive efficiency can be effectively improved. This is a veritable form of active security defense. However, how to accurately depict the attack and attack behavior of the weapon support information network and what kind of camouflage signal to deal with the attack is a complicated problem. Current research results are scarce. A game is a mathematical model to study two competitors' optimal strategies for mutual constraints. It accords with the characteristics of network attack and defense. In recent years, the problem of information security models based on game theory has been paid more and more attention. Literature [1] establishes a mathematical model of attack and defense based on a non-zero-sum attack game. At the same time, the optimal defense decision selection algorithm is given. Literature [2] organically integrates Markov's decision with game theory to understand security situations in equipment support information systems. Literature [3] established a mathematical network attack and defense model based on Bayesian game theory. This paper proposes an information security risk assessment model for complex environments. Literature [4] established a theoretical framework of network attack defense behavior based on the signal countermeasure theory to make the attack defense countermeasure closer to the network reality. Although this method overcomes the shortcoming that the conventional countermeasure requires the joint action of attack and defense, it can only be applied to single-stage attack and defense, not multistage network attack and defense. In this paper, a multilevel signal game model is established. From the perspective of "signal concealment," the active defense problem of the "weapon support information network" is studied. Before facing network security risks, defenders can use hidden signals to trick or deceive attackers to achieve active defense. This is the key to improving China's equipment support information construction level.

2. Complex network security defense diagram.

2.1. Security Defense Diagram.

The defense map is made up of six units, $DG = (R, \xi, R_1, R_2, R_\alpha, R_\beta)$ .R represents the set of nodes on the defense map. Each node represents the state of the network. $\xi \subseteq R \times R$ repre-

[*] Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000 (bgzzzy@ 126.com)

[†] Network Security Management Center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China

[‡] Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000

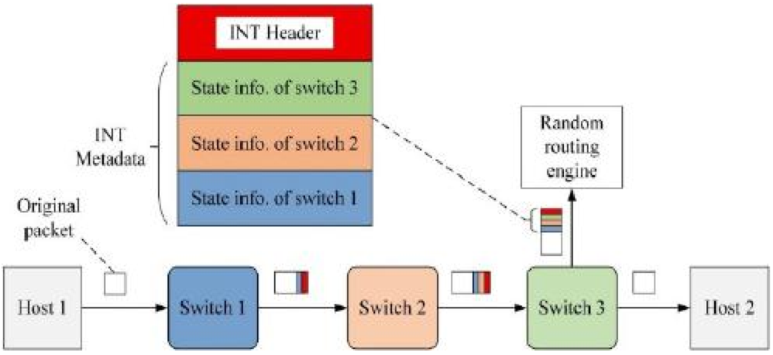

Fig. 2.1: *Randomly generated defense diagram example.*

sents the transitional relationship of the network. $R_1 \subseteq R$ stands for initial network security. $R_2 \subseteq R$ refers to the attack target set. $R_\alpha = (r_1^\alpha, r_2^\alpha, \mathrm{L}, r_m^\alpha)$ stands for strategic mix of objectives. Where $R_\beta = \left(r_1^\beta, r_2^\beta, \mathrm{L}, r_m^\beta\right)$ represents the policy set in the defense system [5]. Defensive maps are one of them. The nodes in the figure cannot only depict the current running status of the network but also reflect the sharing characteristics of the network and the resistance to external attacks. Directed edges describe the change process from one node to another after an atomic attack. R_α represents all of the attacker's attack routes, each an atomic attack [6]. The atomic attack sequence and attack strategy each have their corresponding defense strategies, and these defense measures are combined to form R_β. Figure 2.1 is a randomly generated defense diagram (image cited in Digital Communications and Networks, Volume 8, Issue 3 , June 2022, Pages373-387). In this graph, the directed side represents the transformation of two different security conditions in the corresponding block. $R_\alpha = \{1, 2, 3\}, R_\beta = \left\{r_1^\beta, r_2^\beta, r_3^\beta\right\}$ represents the corresponding defense strategy.

2.2. Creating a Defense Diagram. An attack on a complex network usually causes significant damage to the network. Therefore, it is necessary to take measures such as security detection and security hardening. A defense map is a typical security protection method that can effectively protect it before the attacker attacks it or does not cause heavy losses [7]. In this way, the "passive" information system is transformed into an "active" to achieve the purpose of "high security." The defense chart is detailed in Figure 2.2 (Computers & Security, 2024, 136:103534). The defense diagram contains vital information, such as the data processing and database modules. According to these data, the attacker can search for one or more attack routes to achieve a cost-effectiveness analysis based on offensive and defensive principles and strategies to develop a defensive map.

2.3. Attack and Defense Strategy classification. It is necessary to study the offensive and defensive strategies to achieve accurate network protection [8]. Two aspects should be paid attention to in the division of attack and defense strategies: 1) The complexity of the environment and active defense mode should be comprehensively utilized in establishing the division space of attack and defense strategies. Too much spacing makes the defense mode more complex, while too little spacing makes it difficult for the algorithm to resist various attacks. 2) The attack and defense strategies division must match most current attack patterns. The categories of offensive strategies are listed in Table 2.1.

This project will delve into the types of invasion strategies and the temporal and spatial characteristics of active defense [9]. The defense policies are divided into two categories: host and network. A class contains several subclasses. Details are shown in Table 2.2 and Table 2.3.

DE1 means passive defense. DE2 means medium-strength defense. DE3 stands for active defense. The security protection of complex networks has become the focus of current research [10]. Active defense can conduct security early warning and deep defense and strengthen the defense of information systems to change from passive defense to active defense. This network-based protection method can exclude standard software and trojans. Let users decide whether they can operate or perform a given job according to their wishes.

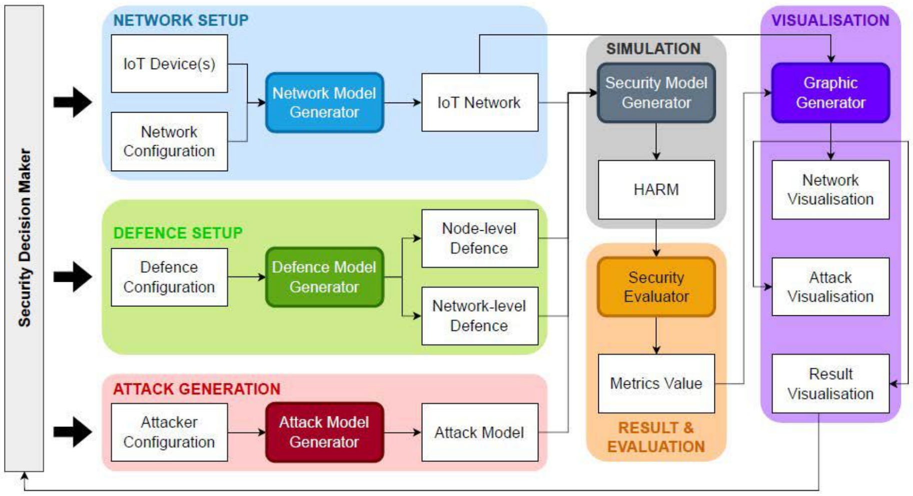

Fig. 2.2: *Defense diagram generation module diagram.*

Table 2.1: *Attack policy classification.*

Sort	Description	Attack lethality
Root	Get Administrator action rights	10
User	Obtain movement permission from network users	5
Data	Illegal access to or reading of data	3
DOS	Denial of service attack	2
Probe	Search attack	0.5
Other	other	*

”Defense” is the process of monitoring and intercepting users, which has a positive protection function for complex network security.

3. Network security active defense model. It is necessary to establish the active protection mode of the information system and choose effective protection measures. When an individual is subjected to a single attack, its protection measures can be optimized at a lower cost. When multiple attack targets are attacked, one attack is effective but ineffective due to the constraints of protection measures [11]. This makes the selection of protective measures more difficult. In this paper, the game theory method is used to solve it. The network security protection diagram $DG = (R, \xi, R_1, R_2, R_\alpha, R_\beta)$ is generated at the input end of the model, and the corresponding optimal protection scheme R_{st} is given. The selection process for face R_{st} is detailed below. 1) Initialize the protection diagram $ADG = (Q_\alpha, Q_\beta), (R_\alpha, R_\beta), (W_\alpha, W_\beta)$. Q_α, Q_β stands for offensive ontology and defensive ontology. W_α, W_β stands for the benefit of attacking and defending agents when appropriate defensive means are used to fend off an attack. 2) If the mode of the offensive and defensive game is $(W_\alpha = -W_\beta)$, only one of W_α, W_β needs to be solved. W_β is used in this paper. 3) r_i^β is the defense in Plan R_β. The defense cost of $r_i^\beta De_{\cos t}(\beta)$ is calculated using formula (3.1):

$$De_{\cos t}(\beta) = E_{\cos t} + M_{\cos t} = E_{\cos t}(\beta) + G_{\cos t} \times s(\alpha, \beta) + B_{\cos t}(\alpha) \times \varepsilon(\alpha, \beta)$$

E_{cost} represents the operational cost of defense. $M_{\cos t}$ stands for passive defensive cost. Y_{cost} stands for remaining defensive strength. G_{cost} represents the cost of adequate system protection. s is a negative defense cost factor. $s(\alpha, \beta)$ describes the adverse consequences of protective action β against the attack mechanism α. $B_{\cos t}(\alpha)$ represents the cost of defending against the actual value β against offensive strategy $\alpha . \varepsilon$ stands for residual loss factor [12]. $\varepsilon(\alpha, \beta)$ is the effect of residual loss on the entire system when protective measure

Table 2.2: Host-based defense policies.

Subclass	Description	Operating cost
End procedure	Close the hacked program or all programs	DE1
Remove file	Delete files that have been changed or attacked	DE1
The account information has been removed	Removal of suspected user account information	DE1
Stoppage service	Terminate programs that are vulnerable to attack	DE2
Restrictions on user movements	Restrict and authorize suspected users	DE2
Shut down the host	Shut down the attacked host	DE2
Restart the host	Restart the attacked host	DE2
Install updater	Update the defective software to the latest version	DE2
Computer virus scanning	Antivirus detection technology	DE3
Document authenticity check	Application software checks the integrity of system files	DE3
Install updater	The system has been updated to the latest	DE3
Reinstall the system	Reinstall the system that was attacked or affected by the virus	DE3
Change account password	Change all system account information	DE2
Set the disk file format	Format the disk and remove the malicious code	DE3
Back-up device	Back-up data	DE3
other	*	*

Table 2.3: *Network-based defense strategies.*

Subclass	Description	Operating cost
Isolated host	Isolate the attacked host from the NIC	DE2
Discard suspicious groupings	Discard suspected packets using IDS or Firewall	DE2
Network outage	Make the attacked system disconnected from the outside world	DE2
TCP reset	Send a reset packet to reset the session	DE2
Blocked port	Close the port through the software	DE2
Blocking IP address	The IP address of the software is blocked. Procedure	DE2
Establishing a black hole path	Use Firewire to change the routing table to an inaccessible IP	DE2
other	*	*

β resists offensive measure α. After the operation, the efficiency function set matrix W is generated, and the index system at each level in the matrix has a close relationship [13]. It's a multilevel index system. The index evaluation and the realistic function comprehensive evaluation of the complex network security active protection mode determine the weight. The evaluation index weight is based on the premise of complex network security. The importance degree of each level factor is evaluated. The result of the composition matrix is as follows:

$$W = [w_{ij}] = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{m1} & w_{m2} & \cdots & w_{mn} \end{bmatrix}$$

w_{ij} represents the degree of subordination to the Class j evaluation set of the Class i use function of the total matrix method index. Evaluation sets integrate views into a complex network security proactive defense model but cannot change the nature of the differences between comments [14]. An evaluation method of attack defense countermeasure based on information entropy is proposed. 4) When the attack and defense strategy mode is $(W_\alpha \neq -W_\beta)$, choose one of the attack plans r_1^α in R_α. Use formula (2.3) to calculate the attack cost of r_1^α $De_{\cos t}(\alpha)$:

$$De_{\cos t}(\alpha) = \sum_{m=1}^{n} G_m \times C_m \times (F_{\cos t} \times Q_i + C_{\cos t} \times Q_c + G_{\cos t} \times Q_v)$$

G_m represents the number of networks attacked. C_m for risk of attack. F_{cost} is the full cost of an attack. Q_i represents the weighted total cost of offense. $C_{\cos t}$ refers to the confidentiality cost of an attack. Q_c is

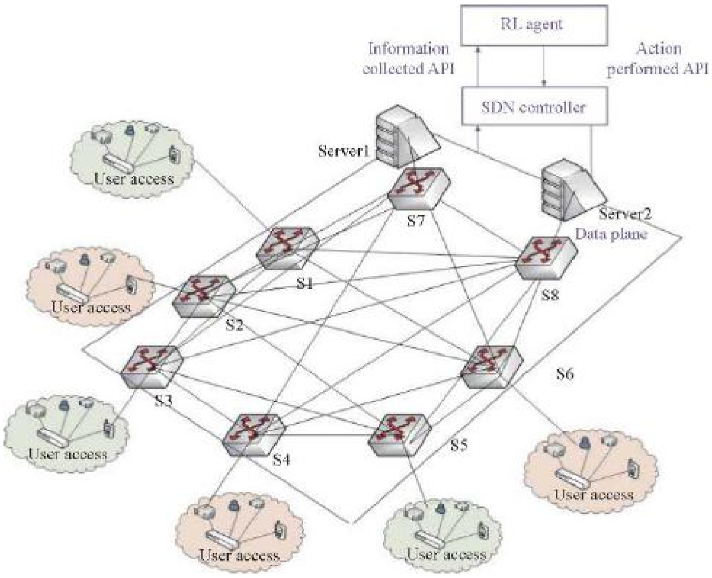

Fig. 4.1: *Network topology of the experimental environment.*

Table 4.1: Attack policy set of the attacker.

Serial number	Attack operation	Cost	Attack strategy	
			Attack 1	Attack 2
Attack 1	Steal the account and crack it	2	Y	Y
Attack 2	Trojan horse activity	3	Y	
Attack 3	Remote buffer overflow	5		Y
Attack 4	Deface a website	4	Y	Y
Attack 5	TCP-SYN flood	7	Y	Y
Attack 6	Oracle TNS listener	6	Y	

weighted by the confidentiality cost of the attack. G_{cost} stands for cost of attack effectiveness. Q_v represents the weighted value of the cost of offensive effectiveness. 5) This paper studies how to choose the target and method of attack. The attacker has local permissions. The attacker must be connected to a host on the target network [15]. The target of the attack can often hit the target in both dimensions of space and time and solve the attack in the fastest and easiest way. To minimize defensive explosion. Choose the best forward defense scheme R_{st} to obtain the best value to establish the active defense mode of the whole complex information system.

4. Simulation experiment and analysis. A test platform is set up to analyze the simulation results. Network security attacks are mainly targeted at external networks. The military firewall insulates the enterprise's internal and external networks. Only a single external host can access the mail server, the network server, and the internal host. Enterprise mail servers, network servers, host servers, and file servers can access the database server [16]. The attacker cannot initially gain direct access to the database but can conduct atomic attacks to achieve this goal. Various network attack programs, such as low Orbit Ion Canon, UDP Flood and Acunetix, are used to automate the test system (fig. 4.1) partially.

The network topology of the attacker is studied, and the attack strategy is obtained. This paper chooses only two ways of attack [17]. It can be seen from Table 4.1 that "Y" represents the offensive actions included in the selected offensive strategy, and the cost of the attack is set according to the difficulty of executing the attack.

According to the difference of defense effectiveness and cost that "defense behavior" may produce, the

Table 4.2: Defense policy set of the defender.

Serial number	Defensive action	Cost	Defensive strategy	
			Defense1	Defense2
Defense1	Delete suspicious accounts	2	Y	Y
Defense2	Restrict packets coming from ports	1	Y	
Defense3	Uninstall and delete Trojan Horse	6	Y	
Defense4	Correct home page	4		Y
Defense5	Repair database	5	Y	Y
Defense6	Restrict SYN/ICMP packets	3	Y	

Table 4.3: Parameters related to attack operations.

Serial number	μ_m	$(W(Z_1), W(Z_2), W(Z_3))$	ε
Attack 1	0.9	(0.7, 0.4, 0.5)	0.1
Attack 2	0.8	(0.5, 0.6, 0.6)	0.4
Attack 3	0.8	(0.5, 0.8, 0.6)	0.4
Attack 4	0.7	(0.5, 0.7, 0.8)	0.3
Attack 5	0.9	(0.4, 0.8, 0.6)	0.3
Attack 6	0.8	(1, 1, 1)	0.4

"defense strategy" database is constructed. Two typical "defense measures" of "high defense" and "weak defense" are selected and studied. The camouflage signal space is $\phi = \{\varphi_1, \varphi_2\}$.φ_1 is high level camouflage. φ_2 is a low-level camouflage signal. Table 4.2 sets out the defense strategy [18]. The "Y" here means that the defense strategy includes the following defense measures, and the defense cost is determined according to the difficulty of defense implementation. When the offensive side chooses the defensive side's strategy, its prior cognition is $(\gamma_1, \gamma_2) = (\gamma_1, 1 - \gamma_1) = (0.3, 0.7)$. The parameters related to offensive operations are listed in Table 4.3.

Use $(10, 15, 15)$ to represent the security attribute value of the Intranet server. Use $(18, 16, 18)$ to indicate the security attribute value of the network service. Use $(20, 20, 22)$ to represent the security property values of the file server. Use $(18, 20, 22)$ to represent the security property values of the file server. Use (25, 28, 30) to represent the security attribute value of the database server. Use $(2, 3; 4, 1)$ indicates the cost of signal hiding [19]. The strategy combination of defense and attack and the corresponding parameters are put forward to get the network defense countermeasure tree. Various information sets are analyzed, and the posterior probability is $p^* = 0.353, q^* = 0.447$. From the process of refined Bayesian Nash equilibrium solution, it can get: $p > p^*, q > q^*$ is $\text{Attack}^*(\varphi_1) = \text{Attack}_1, \text{Attack}^*(\varphi_2) = \text{Attack}_1$, The defender $\varphi^*(\text{Defen }_1) = \varphi_1, \varphi^*(\text{Defen }_2) = \varphi_2$ chooses defense Defens s_1. The defensive option is to hide φ_1, and the offensive option is to attack Attack $_1$. The defender chooses a defensive strategy Defens $_2$. Use the covert signal " φ_1 " as a defense [20]. The attacker adopts the offensive strategy Attack $_1$. The refined Bayesian Nash equilibrium is the confusion equilibrium $S_1 = \{(\varphi_1, \varphi_1) \to (\text{ Attack }_1, \text{ Attack }_1), p = \gamma_1, q > q^*\}$. The paper studies the refined Bayesian Nash equilibrium for other cases.

When $p > p^*, q > q^*$ is the mixed equilibrium, call it $S_2 = \{(\varphi_1, \varphi_2) \to (\text{ Attack}_1, \text{Attack }_1), p = \gamma_1, q > q^*\}$.

When $p < p^*, q > q^*$ is the separate equilibrium, call it $S_3 = \{(\varphi_2, \varphi_1) \to (\text{ Attack}_2, \text{Attack }_1), p = 0, q = 1\}$.

When $p < p^*, q < q^*$ is the mixed equilibrium, call it $S_4 = \{(\varphi_1, \varphi_1) \to (\text{ Attack}_2, \text{Attack }_2), p = \gamma_1, q > q^*\}$ For $\gamma_1 = 0.3 < p^*, \gamma_2 = 0.7 > q^*$, then, the refined Bayesian Nash equilibrium B is proper. In terms of defense, the high level of defense plan Defens s_1 chooses the lower level of covert signal φ_2. The benefit is most significant when the higher cover signal φ_1 is chosen in the weaker defense strategy Defens $_2$. Turning a low-level defense into an advanced one can keep attackers at bay. The choice of the covert signal can effectively enhance the secrecy performance of the military intelligence system so that it can better play its active defense role.

5. Conclusion. This paper analyzes the attack and defense of military intelligence networks and proposes the optimal choice scheme of camouflage signal based on game theory. Simulation results show that the algorithm can be applied to the covert system to achieve active network defense. Therefore, enhancing the security protection level of our military information network is of great practical significance.

REFERENCES

[1] Zhu, M., Anwar, A. H., Wan, Z., Cho, J. H., Kamhoua, C. A., & Singh, M. P. (2021). A survey of defensive deception: Approaches using game theory and machine learning. IEEE Communications Surveys & Tutorials, 23(4), 2460-2493.

[2] Li, X. (2022). An evolutionary game-theoretic analysis of enterprise information security investment based on information sharing platform. Managerial and Decision Economics, 43(3), 595-606.

[3] Shao, C. W., & Li, Y. F. (2021). Optimal defense resources allocation for power system based on bounded rationality game theory analysis. IEEE Transactions on Power Systems, 36(5), 4223-4234.

[4] Li, X. (2021). Decision making of optimal investment in information security for complementary enterprises based on game theory. Technology Analysis & Strategic Management, 33(7), 755-769.

[5] Liu, B., Su, Z., & Xu, Q. (2021). Game theoretical secure wireless communication for UAV-assisted vehicular Internet of Things. China Communications, 18(7), 147-157.

[6] Luo, S., & Choi, T. M. (2022). E-commerce supply chains with considerations of cyber-security: Should governments play a role. Production and Operations Management, 31(5), 2107-2126.

[7] Tsemogne, O., Hayel, Y., Kamhoua, C., & Deugoué, G. (2021). Game-theoretic modeling of cyber deception against epidemic botnets in internet of things. IEEE Internet of Things Journal, 9(4), 2678-2687.

[8] Lakshminarayana, S., Belmega, E. V., & Poor, H. V. (2021). Moving-target defense against cyber-physical attacks in power grids via game theory. IEEE Transactions on Smart Grid, 12(6), 5244-5257.

[9] Xu, S., Yung, M., & Wang, J. (2021). Seeking Foundations for the Science of Cyber Security: Editorial for Special Issue of Information Systems Frontiers. Information Systems Frontiers, 23(2), 263-267.

[10] Liu, S. Z., Shao, C. W., Li, Y. F., & Yang, Z. (2021). Game attack–defense graph approach for modeling and analysis of cyberattacks and defenses in local metering system. IEEE Transactions on Automation Science and Engineering, 19(3), 2607-2619.

[11] Gouissem, A., Abualsaud, K., Yaacoub, E., Khattab, T., & Guizani, M. (2021). Game theory for anti-jamming strategy in multichannel slow fading iot networks. IEEE Internet of Things Journal, 8(23), 16880-16893.

[12] Arisdakessian, S., Wahab, O. A., Mourad, A., Otrok, H., & Guizani, M. (2022). A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions. IEEE Internet of Things Journal, 10(5), 4059-4092.

[13] Cheng, L., Yan, H., Zhan, X., Fan, S., & Shi, K. (2021). Stability analysis of networked control systems under DoS attacks in frequency domain via game theory strategy. International Journal of Systems Science, 52(14), 2934-2946.

[14] Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. Artificial Intelligence Review, 55(7), 5215-5261.

[15] Abou El Houda, Z., Brik, B., Ksentini, A., Khoukhi, L., & Guizani, M. (2022). When federated learning meets game theory: A cooperative framework to secure iiot applications on edge computing. IEEE Transactions on Industrial Informatics, 18(11), 7988-7997.

[16] Balcaen, P., Bois, C. D., & Buts, C. (2022). A game-theoretic analysis of hybrid threats. Defence and Peace Economics, 33(1), 26-41.

[17] Wan, M., Li, J., Liu, Y., Zhao, J., & Wang, J. (2021). Characteristic insights on industrial cyber security and popular defense mechanisms. China Communications, 18(1), 130-150.

[18] Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5), 1-36.

[19] Ferrag, M. A., Shu, L., Friha, O., & Yang, X. (2021). Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. IEEE/CAA Journal of Automatica Sinica, 9(3), 407-436.

[20] Soussi, W., Christopoulou, M., Xilouris, G., & Gür, G. (2021). Moving target defense as a proactive defense element for beyond 5G. IEEE Communications Standards Magazine, 5(3), 72-79.

Edited by: Zhigao Zheng
Special issue on: Graph Powered Big Aerospace Data Processing
Received: Nov 23, 2023
Accepted: Dec 15, 2023