3-2023

Military and Security Applications: Cybersecurity (Encyclopedia of Optimization, Third Edition)

Nathaniel D. Bastian
Army Cyber Institute, U.S. Military Academy, nathaniel.bastian@westpoint.edu

Matthew Dinmore

M

Military and Security Applications: Cybersecurity

Nathaniel D. Bastian[1] and Matthew D. Dinmore[2]
[1]Army Cyber Institute, United States Military Academy, West Point, NY, USA
[2]Johns Hopkins University Applied Physics Laboratory, Laurel, MD, USA

Article Outline

Keywords

Cybersecurity · Stochastic optimization · Discrete optimization · Continuous optimization

MSC Codes

65K05, 74P99, 78M50, 90C05, 90C10, 90C11, 90C15, 90C26, 90C27, 90C29, 90C30, 90C90

Introduction

The domain of cybersecurity is growing as part of broader military and security applications, and the capabilities and processes in this realm have qualities and characteristics that warrant using solution methods in mathematical optimization. Problems of interest may involve continuous or discrete variables, a convex or nonconvex decision space, differing levels of uncertainty, and constrained or unconstrained frameworks. Cyberattacks, for example, can be modeled using hierarchical threat structures and may involve decision strategies from both an organization or individual and the adversary. Network traffic flow, intrusion detection and prevention systems, interconnected human-machine interfaces, and automated systems – these all require higher levels of complexity in mathematical optimization modeling and analysis [18]. Attributes such as cyber resiliency, network adaptability, security capability, and information technology flexibility – these require the measurement of multiple characteristics, many of which may involve both quantitative and qualitative interpretations. And for nearly every organization that is invested in some cybersecurity practice, decisions must be made that involve the competing objectives of cost, risk, and performance [18]. As such, mathematical optimization has been widely used and accepted to model important and complex decision problems, providing analytical evidence for

P. M. Pardalos, O. A. Prokopyev (eds.), *Encyclopedia of Optimization*,
https://doi.org/10.1007/978-3-030-54621-2_761-1

helping drive decision outcomes in cybersecurity applications [18].

In the paragraphs that follow, this entry highlights a small portion of recent mathematical optimization research in the body of knowledge applied to the cybersecurity space. The subsequent literature discussed fits within a broader cybersecurity domain taxonomy considering the categories of analyze, collect and operate, investigate, operate and maintain, oversee and govern, protect and defend, and securely provision. The scope of this entry does not include the application of optimization to the design of cyberphysical systems; while not covered here, Enayaty-Ahangar, Albert, and DuBuis [12] provide a systematic review of the literature applying optimization to enhance or improve cyberinfrastructure security, highlighting application areas, mission areas, and optimization models and methods. Further, the paragraphs are structured around generalized mathematical optimization categories to provide a lens to summarize the existing literature, including uncertainty (stochastic programming, robust optimization, etc.), discrete (integer programming, multiobjective, etc.), continuous-unconstrained (nonlinear least squares, etc.), continuous-constrained (global optimization, etc.), and continuous-constrained (nonlinear programming, network optimization, linear programming, etc.). At the conclusion of this chapter, research implications and extensions are offered to the reader that desires to pursue further mathematical optimization research for cybersecurity within a broader military and security applications context.

Optimization Under Uncertainty

For the mathematical optimization category of uncertainty, stochastic programming and robust optimization approaches are the most common approaches applied to the cybersecurity domain. Paul and Zhang [25]. study the decision-making problem in cybersecurity risk planning concerning resource allocation strategies by government and firms. Aiming to minimize the social costs incurred due to cyberattacks, the authors consider not only the monetary investment costs but also the deprivation costs due to detection and containment delays. The optimal decision guides the firms on the countermeasure portfolio mix (detection vs. prevention vs. containment) and government intelligence investments while accounting for actions of a strategic attacker and firm budgetary limitations. The authors accomplish this via a two-stage stochastic programming model. In the first stage, firms decide on prevention and detection investments aided by government intelligence investments that improve detection effectiveness. In the second stage, once the attacker's actions are realized, firms decide on containment investments after evaluating the cyberattacks.

A related cybersecurity investment problem is tackled by Zheng, Albert, Luedtke, and Towle [36], who study how to identify strategies for mitigating cyberinfrastructure vulnerabilities. They propose an optimization framework that prioritizes the investment in security mitigations to maximize the coverage of vulnerabilities. They use multiple coverage to reflect the implementation of a layered defense, and they consider the possibility of coverage failure to address the uncertainty in the effectiveness of some mitigations. They design greedy approximation algorithms for identifying near-optimal solutions to the models. The computational study suggests that their models yield robust solutions that use a layered defense and provide an effective mechanism to hedge against the risk of possible coverage failure. This work is later expanded upon by Zheng and Albert [35] in the robust optimization context, who extend existing stochastic expected budgeted maximum multiple coverage models that identify "good" solutions on average that may be unacceptable in certain circumstances. The proposed three alternative robust optimization models that consider different robustness methods that hedge against worst-case risks, including models that maximize the worst-case coverage, minimize the worst-case regret and maximize the average

coverage in the $(1 - \alpha)$ worst cases (conditional value at risk). Their study provides valuable tools and insights for decision-makers with different risk attitudes to manage cybersecurity risks under uncertainty.

Discrete Optimization

The use of discrete optimization approaches is heavily leveraged in the cybersecurity applications, particularly mixed-integer programming, multiple objective optimization, and more general combinatorial optimization. For example, Sawik [26] explores the optimal selection of countermeasures in information technology (IT) security planning to prevent or mitigate cyberthreats. Given a set of potential threats and a set of available countermeasures, the decision-maker needs to decide which countermeasure to implement under limited budget to minimize potential losses from successful cyberattacks and mitigate the impact of disruptions caused by IT security incidents. The selection of countermeasures is based on their effectiveness of blocking different threats, implementation costs, and probability of potential attack scenarios. The problem is formulated as a single- or biobjective mixed integer program, and a conditional value-at-risk approach combined with scenario-based analysis is applied to control the risk of high losses due to operational disruptions and optimize worst-case performance of an IT system. Following this work, Sawik [27]. presents a mixed-integer linear programming formulation for optimization of cybersecurity investment in Industry 4.0 supply chains. Using a recursive linearization procedure, a complex nonlinear stochastic combinatorial optimization model with a classical exponential function of breach probability is transformed into its linear equivalent. The obtained linear optimization model is capable of selecting optimal portfolio of security safeguards to minimize cybersecurity investment and expected cost of losses from security breaches in a supply chain.

In addition to using optimization for IT cybersecurity planning and investment decision-making, Khouzani, Liu, and Malacaria [19] present a framework to efficiently solve a multiobjective optimization problem for cyber-security defense. Facing an attacker who can mount a multistage attack (modeled using attack graphs), the defense problem is to select a portfolio of security controls which minimizes the security risk and the (direct and indirect) costs of the portfolio of controls. The authors model the problem as a min-max multiobjective optimization. Furthermore, Altunay, Leyffer, Linderoth, and Xie [3] consider how to optimally respond to attacks in open grid environments. The authors first discuss how collaborations manifest themselves in the grids and form the collaboration network graph, and how this collaboration network graph affects the security threat levels of grid participants. They present two mixed-integer program models to find the optimal response to attacks in open grid environments, and they also calculate the threat level associated with each grid participant. Given an attack scenario, their optimal response model aims to minimize the threat levels at unaffected participants while maximizing the uninterrupted scientific production (continuing collaborations). Additional work on grid-related optimization for cybersecurity is done by Arguello, Johnson, and Gearhart [5], who develop a novel trilevel mathematical programming model to optimally segment a grid communication system, taking into account the actions of an IT administrator, attacker, and grid operator. The IT administrator is given an allowance to segment existing networks, and the attacker is given a fixed budget to attack the segmented communication system in an attempt to inflict damage on the grid. Finally, the grid operator is allowed to redispatch the grid after the attack in order to minimize damage. The resulting problem is a trilevel interdiction problem, which the authors solve by leveraging current research in bilevel branch and bound.

Another heavily researched cybersecurity area involves the cybersecurity operations center. Shah, Ganesan, Jajodia, and Cam [28] investigate the problem of allocating clusters of sensors to analysts for investigation within a cybersecurity operations center. There are two essential

properties that must be met in the above grouping and allocation process: 1) meeting the cluster's requirement for specific analyst expertise mix, complete tool coverage that allows the analysts to handle the type of alerts generated, and analyst credentials such as security clearances; and 2) minimizing and balancing the number of unanalyzed alerts among clusters at the end of the daily work shift because an imbalance or a large number of unanalyzed alerts among clusters due to factors such as lack of analyst credentials or tooling expertise in a cluster would pose a security risk to the organization. The authors model and solve this resource allocation problem using mixed-integer programming. Ganesan, Jajodia, and Shah [15] employ reinforcement learning-based stochastic dynamic programming optimization model that incorporates estimates of future cyber alert rates and responds by dynamically scheduling cybersecurity analysts to minimize risk (i.e., maximize significant alert coverage by analysts) and maintain the risk under a predetermined upper bound. The authors test the dynamic optimization model and compare the results to an integer programming model that optimizes the static staffing needs based on a daily-average alert generation rate with no estimation of future alert rates (static workforce model). Ganesan, Jajodia, and Cam [14] present a generalized optimization model using mixed-integer-programming for scheduling cybersecurity analysts to minimize risk (a.k.a., maximize significant alert coverage by analysts) and maintain risk under a predetermined upper bound. The article tests the optimization model and its scalability on a set of given sensors with varying analyst experiences, alert generation rates, system constraints, and system requirements. Finally, Shah, Ganesan, Jajodia, and Cam [29] present a novel two-step sequential mixed integer-programming optimization method that is used in the development of a new decision-support business model for outsourcing the alert analysis process. It is demonstrated that through this model, a cybersecurity operations center can effectively deliver its alert management services.

Continuous-Unconstrained Optimization

Continuous, unconstrained optimization techniques are often used in cybersecurity modeling to help reduce noise and find the desired signal of malicious activities in various types of sensor and network data. This is especially challenging due to the large imbalance between benign (normal) network traffic and malicious traffic. A particularly common class of methods are evolutionary, biologically inspired approaches, especially particle swarm optimization (PSO). Thakkar and Lohiya [32] offer a recent survey that includes discussion of these methods in general as applied to the problem if intrusion detection. Nayak, Vakula, Dinesh, and Naik [23] review a decade of work in PSO methods for intrusion detection. They note three major classes of applications: traditional PSOs, PSOs modified to the intrusion detection problem, and hybrid PSOs, in which PSOs are combined with other machine learning methods, often employing the PSOs to optimize the weights or parameters for the other methods. Alyasiri, Clark, and Kudenko [4] consider the application of evolutionary computing methods to cyberattack detection. After reviewing genetic programming and grammatical evolutionary approaches, they introduce a novel Cartesian Genetic Programming (CGP) approach. They choose this methodology in part due to its ability to avoid generating solution code that has no effect on fitness, but must be run nonetheless, thereby reducing runtime performance. They employ a supervised training method for the three evolutionary computing methods against labeled examples of malicious and benign behavior, notably across a range of cybersecurity-relevant datasets including phishing and network data. The results of their experiments demonstrate that the CGP approach performs as well or better than the other evolutionary computing methods in terms of detection rate, false alarm rate, and overall accuracy. Chohra, Debbabi, and Shirani [9] incorporate a particle swarm optimization method as part of their Daedalus network anomaly detection system, which

analyzes intrusion detection system logs. In particular, they apply PSO to the challenging problem in analyzing cybersecurity network data of distinguishing malicious activity-induced anomalies from normal network noise. Applying this to the time series data from the network, they are able to remove period effects that would otherwise trigger the anomaly detection logic. As compared to a baseline k-means anomaly detection, their system was able to significantly improve accuracy and combined precision and recall as measured by the F1 score, while also demonstrating considerably better (approximately 5x) execution time. Ghanem and Jantan [16] also employ swarm methods, in this case a hybrid of bioinspired methods based on an artificial bee colony (ABC) and Monarch butterfly optimization (MBO) behaviors. The methods are used in a complementary fashion, exploiting the MBO algorithm's efficiency in exploring the overall search space, while making up for its weakness in finding local optima by employing the ABC algorithm. Together, these are used to optimize an artificial neural network (ANN) that serves as a classifier for network packets, labeling them either malicious or benign. Evaluated against multiple datasets, the proposed hybrid approach consistently outperforms either of the methods independently, or a variety of other similar optimization methods in terms of detection rate, false alarm rate, and overall accuracy.

Ghanem and Jantan [17] have similarly explored the use of a bat algorithm to optimize the weights for a multilayer perceptron model, also finding better performance than similar methods. In both experiments, the authors note that these results are obtained in the absence of a feature selection method, the incorporation of which should serve to further improve performance. A similar application is found in Davahli, Shamsi, and Abaei [10] who report on the use of a combined genetic algorithm and gray wolf optimization algorithm to identify the most effective features in network traffic to use in training a support vector machine-based intrusion detector for wireless Internet-of-Things (IoT) networks. They find the main benefit of this hybrid approach is in lower computational time due to reduced dimensionality of the feature set, with detection performance being the same or slightly degraded, suggesting that feature optimization is a useful approach for low-power/compute applications such as IoT. Benmessahel, Xie, Chellal, and Semong [6] apply the locust swarm metaheuristic optimization algorithm in a similar manner to optimize a feed-forward neural network (FNN) for intrusion detection. They compare this approach to optimizing the FNN with both a genetic algorithm and a particle swarm optimizer, finding that the locust swarm is superior in all performance measures across a range of network cyberattack types. In a comparable application for smart grid security against cyberattack, Deng, Zhou, Yue, Hu, and Zhu [11] employ a hybrid gene expression cloud-programming approach that is used to deal with high-dimensional netflow data, and also develop a nonlinear least squares model for intrusion detection. Gene expression programming is used as a multiclassification methodology against log data that has been preprocessed with an attribute reduction algorithm based on rough sets to reduce noise. The resulting gene expression algorithm produces local intrusion detection function models, which are then combined into a nonlinear least squares-based global intrusion detection model. The authors conduct experiments against several well-known datasets with multiple attack types, finding that the approach is more sensitive with respect to small sample sizes, and provides better overall runtime performance over previous gene expression-programming approaches to intrusion detection. Finally, Alhajjar, Maxwell, and Bastian [2] have used evolutionary techniques in the generation of adversarial examples for machine learning in network intrusion detection applications. They develop GA, PSO, and deep learning-based (Generative Adversarial Networks, GANs) methods and apply them against machine learning-based intrusion detection systems. Among their findings were that certain classifiers (based on support vector machines and decision trees) were highly susceptible to all three

adversarial generators. They also found that adversarial examples that tend to evade one classifier also tend to evade the others.

Beyond intrusion detection, PSO has found other cybersecurity applications. For example, Chen, Wang, Zhang, and Xu [8] have used PSOs for phishing detection, that is, attempts to lure individuals to click on a link or take some other action that results in enabling an intrusion. They use the classic particle swarm algorithm to optimize the weights for a back propagation (BP) neural network based on features extracted from phishing uniform resource locator (URL) strings. Evaluating the model against a collection of legitimate and phishing website URLs, the authors find the PSO-optimized neural network achieves modest improvements in performance over a nonoptimized BP neural network in terms of accuracy, precision, recall, and false negative rate, while also achieving faster convergence in model training. Tayal and Ravi [31] also apply optimization to phishing detection. They use binary particle swarm optimization to conduct fuzzy association rule mining on transactional data. The data are first converted to a fuzzy format, and then the swarm optimization is run repeatedly, each time generating a best fuzzy association rule. Due to the evolutionary nature of the method, it is likely that different rules will be generated in each run, creating an ensemble of well-fit rules that can be applied to emails to score them. In evaluating the approach, the authors found the binary particle swarm-optimized algorithm produced superior rules to those generated by fuzzy association mining alone as measured comparatively using the same fitness function.

In another example of the application of optimization methods to noise reduction, Won and Bertino [33] address the problem of attacker-introduced position information in wireless sensor networks that can affect typically robust Minimum Mean Square Estimation (MMSE) methods that are used to estimate optimal sensor positioning. The authors' "Inside-Attack" novel technique is demonstrated to introduce significant errors into MMSE estimates, given that the attacker knows the locations of the sensors. They then define the Inside-Attack Filtering (IAF) algorithm as a proposed defense against this attack, which they implement as IAF-MMSE and evaluate via simulation. Their results demonstrate that, even as malicious position information is increased, IAF-MMSE maintains stable position estimation errors as a result of filtering out the malicious inputs, while prior MMSE-based methods all degrade in accuracy, though, as they uncover, each for different reasons. Bernal Alzate, Lancheros-Cuesta, and Huang [7] consider another type of noise that which may be intentionally injected by an attacker to mislead attack detection. Focusing on smart grids, they advance a distributed state estimate methodology that leverages a limited number of observations from system monitors, such as smart meters. To avoid ill-conditioning, the authors utilize the Levenberg-Marquardt method, which they have extended for state estimation in the case of smart grids. They address the potential case where communications with smart meters are lost or false data is injected into the system by the attacker, resulting in too few inputs to solve the system. To overcome this, the method also uses the readings from the slack node at transformer stations, which offer sufficient redundancy to assure solvability. Through this approach, the ability to detect attacks even with a 10% reduction in data due to the attack or failures is demonstrated.

The wide range of cyber networking environments offer other challenges that can be addressed through optimization. Also considering evolutionary methods, Kusyk, Uyar, and Sahin [20] survey their application to mobile ad hoc networks (MANETs). These networks are particularly vulnerable because they are highly dynamic inasmuch as they are created on-the-fly between mobile devices, thus increasing the need for intrusion detection and other cybersecurity measures. The authors find that a range of evolutionary methods, including genetic programming, particle swarm optimization, and artificial immune systems, had been applied to different degrees for MANET cybersecurity both due to their inherent ability to adapt as well as their relatively lightweight implementations, which

are essential in low-power environments. They discuss evolutionary game theory as a framework for employing these methods for MANETs; the elimination of a rationality requirement allows for a dynamic game arrangement, which is well-fit to MANET-specific applications of intrusion detection, cryptosystems, and trust and reputation establishment in a network.

Continuous-Constrained Optimization

Continuous, constrained optimization techniques find multiple applications in cybersecurity. A significant area of research has been in creating optimization models to assist network defenders in making cybersecurity investments or managing defenses with limited resources. As an example, Nagurney and Shukla [22] develop and compare several distinct models for cybersecurity investment in competitive and cooperative situations to safeguard against potential and ongoing threats. The authors introduce a Nash equilibrium model of noncooperation in terms of cybersecurity levels of the firms involved, which is formulated, analyzed, and solved using variational inequality theory. Nash bargaining theory is utilized to argue for information sharing and to quantify its monetary and security benefits in terms of reduction in network vulnerability to cyberattacks. A final model focuses on cooperation among the firms in terms of their cybersecurity levels, but from a system-optimization perspective in which the sum of the expected utilities is maximized. Nisioti, Loukas, Laszka, and Panaousis [24] present DISCLOSE, a data-driven decision support framework using constrained optimization techniques for optimizing forensic investigations of cybersecurity breaches. DISCLOSE benefits from a repository of known adversarial tactics, techniques, and procedures (TTPs), for each of which it harvests threat intelligence information to calculate its probabilistic relations with the rest. These relations, as well as a proximity parameter derived from the projection of quantitative data regarding the adversarial TTPs on an attack life cycle model, are both used as input to the author's optimization framework. Yamany, Moustafa, and Turnbull [34] introduce a trilevel programming framework to assist in modeling attacks and defenses against a smart power grid toward optimizing defense investments and employments. Structured as an upper-level defensive player minimization problem against a hierarchical, lower-level, attacker-operator maximization problem, the authors develop a mixed-integer nonlinear programming approach. They use a genetic algorithm embedded with column and constrained generation (C&CG) to solve the linked problems. Their simulations reflect an improvement over previous models in unmet demand management, while also revealing that attackers prefer attacks that cause cascading effects.

In another application, researchers have developed models to assist in generating network management policies that balance utility with security. Modern networks often leverage software to dynamically define or reconfigure the network, which would potentially require adjusting security policies for a new configuration. Examining this, Achleitner, Burke, McDaniel, Jaeger, La Porta, and Krishnamurthy [1] apply network optimization methods to determine a balanced, optimal, multilevel security policy for a software-defined network. They achieve a balance of goals with two models: one that determines a security policy-based network (implemented as discrete rules that serve as constraints), and another that finds the minimal security cost in relaxing the policies to ensure all desired network flows are routable. To maximize flows within the given constraints, they augment a binary integer-programming model with a modified shortest-path heuristic to make computation tractable. The relaxation model uses integer-linear programming to minimize a security cost metric they develop. Their evaluation on two representative network models (data center and enterprise network designs) finds that 85–87% optimal security coverage is achieved. Solution generation time is critical because, as a software-defined network, rapid reconfiguration is expected. They demonstrate that a typical solver scales in a power law

relationship to the number of nodes, while their heuristic approach scales more effectively.

Furthering the examination of the relationship between business utility and security, Stergiopoulos, Dedousis, and Gritzalis [30] approach the network optimization problem for security by looking at the interconnectivity of business process assets (that is, things of value to a corporation) and devices as a network optimization problem. By assigning priorities to the assets and their associations via networked devices, they are able to then assess risk as a measure on the resulting graph's dependency paths. Applying a minimum spanning tree algorithm optimally restructures the network, which is then clustered to create subnetworks. Their results demonstrate that this approach can minimize risk; however, as they note, there is an assumption of both a good understanding of the business assets and their relative values for the risk model, as well as the mapping of those assets to the cyber infrastructure, both of which may be challenging to achieve and maintain in a large enterprise.

Optimization can be used to assist defenders (and, to a degree, attackers) in selecting strategies for employing cyber capabilities during an attack; these often leverage game theory to seek equilibrium conditions for both players (attackers and defenders) under the assumption of limited resources. For example, Liu, Feng, Lian, Chen, and Zhang [21] present a Bayesian game model for analyzing attack and defense strategies for distributed denial of service (DDoS) attacks. For the attacker, they choose the most common strategy seen in practice (essentially an outsourced, mass-attack service), while for the defender they employ a nonlinear programming model to represent the various defense strategies (increasing network bandwidth, deploying a DDoS filter, or acquiring insurance), all of which have differing costs and which may be employed in combinations, to find an optimal defense strategy toward achieving Nash equilibrium in the game. In simulations, they find that the approach effectively finds solutions that can assist network owners in making defensive investments.

As noted earlier, a particular challenge in cybersecurity arises when the attacker intentionally targets cybersecurity systems including sensors or algorithms intended to assist defenders. Making these systems robust to attack such as false data injection or denial-of-service (DoS) is another application for optimization techniques. In an example of this, Feng and Hu [13] address a resilient exponential distributed convex optimization problem for a heterogeneous linear multiagent system under DoS attacks over random digraphs. Two types of time-based and event-based resilient distributed optimization algorithms were proposed by the authors to solve these problems, respectively. Under both algorithms, the global minimizer was achieved exponentially, provided that an explicit analysis of the frequency and duration of attacks was established. In addition, it was proved that there were no Zeno behavior occurring under the dynamic event-triggered condition.

Conclusion

Cybersecurity is an asymmetric conflict; the attacker only needs to be successful once, and the defender usually cannot afford to defend everything. As a result of this imbalance, defenders must seek to optimally employ cybersecurity resources, whether defensive measures, analysts, or computational capabilities. As is evident in the brief preceding survey, examples of applications of the full range of optimization methods to cybersecurity are readily found in the literature. Key application areas include informing policy decisions for the allocation of cyberdefensive investments and resources given likely attacks and attack motives. These are decisions often driven by cost minimization, and several solutions incorporate game theory toward finding attacker defender equilibria. Similarly, the methods for the selection of defensive tactics that minimize attack cost are presented in several papers. Optimizing cybersecurity operations and resources has also been investigated resulting in methods to manage analysts and capabilities.

Significant research has been done in attack detection, involving major cybersecurity data types and significant attack vectors including

network intrusion and phishing detection. Optimization methods are often applied to find optimal sets of features for subsequent model training, with the application of particle swarm optimization as a preparatory layer for training machine-learning classifiers, a particularly common approach.

From the perspective of the landscape of cybersecurity, while many of principal areas have benefited from optimization research, there are several areas that have not had significant attention and may warrant further research, including data collection, retention, and analysis optimization; malware detection, classification, and management; cyberoperational planning; and the conduct of cyber investigations and digital forensics. Also essential will be the translation of these research results into operations, which will require them to first be evaluated and characterized under real-world conditions, and then incorporated seamlessly into the tools, methods, and training utilized by cybersecurity practitioners.

See also

- ▸ Military and Security Applications: Behavioral Modeling
- ▸ Military and Security Applications: Medical Evacuation

References

1. Achleitner S, Burke Q, McDaniel P, Jaeger T, La Porta T, Krishnamurthy S (2020) MLSNet: a policy complying multilevel security framework for software defined networking. arXiv:2009.10021 [cs]
2. Alhajjar E, Maxwell P, Bastian N (2021) Adversarial machine learning in network intrusion detection systems. Expert Syst Appl 186:115782. https://doi.org/10.1016/j.eswa.2021.115782
3. Altunay M, Leyffer S, Linderoth JT, Xie Z (2011) Optimal response to attacks on the open science grid. Comput Netw 55:61–73. https://doi.org/10.1016/j.comnet.2010.07.012
4. Alyasiri H, Clark JA, Kudenko D (2019) Evolutionary computation algorithms for detecting known and unknown attacks. In: Lanet J-L, Toma C (eds) Innovative security solutions for information technology and communications. Springer International Publishing, Cham, pp 170–184
5. Arguello B, Johnson ES, Gearhart JL (2021) A trilevel model for segmentation of the power transmission grid cyber network. arXiv:2108.10958 [math]
6. Benmessahel I, Xie K, Chellal M, Semong T (2019) A new evolutionary neural networks based on intrusion detection systems using locust swarm optimization. Evol Intel 12:131–146. https://doi.org/10.1007/s12065-019-00199-5
7. Bernal Alzate E, Lancheros-Cuesta D, Huang Z (2021) Cyber-attack mitigation on low voltage distribution grids by using a novel distribution system state estimation approach. In: Cortes Tobar DF, Hoang Duy V, Trong Dao T (eds) AETA 2019 – recent advances in electrical engineering and related sciences: theory and application. Springer International Publishing, Cham, pp 107–116
8. Chen W, Wang XA, Zhang W, Xu C (2018) Phishing detection research based on PSO-BP neural network. In: Barolli L, Xhafa F, Javaid N, Spaho E, Kolici V (eds) Advances in internet, data & web technologies. Springer International Publishing, Cham, pp 990–998
9. Chohra A, Debbabi M, Shirani P (2019) Daedalus: network anomaly detection on IDS stream logs. In: Zincir-Heywood N, Bonfante G, Debbabi M, Garcia-Alfaro J (eds) Foundations and practice of security. Springer International Publishing, Cham, pp 95–111
10. Davahli A, Shamsi M, Abaei G (2020) Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks. J Ambient Intell Human Comput 11:5581–5609. https://doi.org/10.1007/s12652-020-01919-x
11. Deng S, Zhou A, Yue D, Hu B, Zhu L (2017) Distributed intrusion detection based on hybrid gene expression programming and cloud computing in a cyber physical power system. IET Control Theory Appl 11:1822–1829. https://doi.org/10.1049/iet-cta.2016.1401
12. Enayaty-Ahangar F, Albert LA, DuBois E (2021) A survey of optimization models and methods for cyberinfrastructure security. IISE Trans 53:182–198. https://doi.org/10.1080/24725854.2020.1781306
13. Feng Z, Hu G (2021) Attack-resilient distributed convex optimization of linear multi-agent systems against malicious cyber-attacks over random digraphs. arXiv:2105.02423 [cs, eess, math]
14. Ganesan R, Jajodia S, Cam H (2017) Optimal scheduling of cybersecurity analysts for minimizing risk. ACM Trans Intell Syst Technol 8:1–32. https://doi.org/10.1145/2914795
15. Ganesan R, Jajodia S, Shah A, Cam H (2016) Dynamic scheduling of cybersecurity analysts for minimizing risk using reinforcement learning. ACM Trans Intell Syst Technol 8:1–21. https://doi.org/10.1145/2882969
16. Ghanem WAHM, Jantan A (2020) Training a neural network for cyberattack classification appli-

cations using hybridization of an artificial Bee colony and Monarch butterfly optimization. Neural Process Lett 51:905–946. https://doi.org/10.1007/s11063-019-10120-x
17. Ghanem WAHM, Jantan A (2020) A new approach for intrusion detection system based on training multilayer perceptron by using enhanced Bat algorithm. Neural Comput & Applic 32:11665–11698. https://doi.org/10.1007/s00521-019-04655-2
18. Goethals P, Scala N, Bastian N (2022) Operations research. In: Bennett D, Goethals P, Scala N (eds) Mathematics in cyber research. CRC Press, Boca Raton, pp 233–266
19. Khouzani M, Liu Z, Malacaria P (2019) Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. Eur J Oper Res 278:894–903. https://doi.org/10.1016/j.ejor.2019.04.035
20. Kusyk J, Uyar MU, Sahin CS (2018) Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks. Evol Intel 10:95–117. https://doi.org/10.1007/s12065-018-0154-4
21. Liu Y, Feng D, Lian Y, Chen K, Zhang Y (2013) Optimal defense strategies for DDoS defender using Bayesian game model. In: Deng RH, Feng T (eds) Information security practice and experience. Springer, Berlin/Heidelberg, pp 44–59
22. Nagurney A, Shukla S (2017) Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. Eur J Oper Res 260:588–600. https://doi.org/10.1016/j.ejor.2016.12.034
23. Nayak J, Vakula K, Dinesh P, Naik B (2020) Significance of particle Swarm optimization in intrusion detection: crossing a decade. In: Nayak J, Balas VE, Favorskaya MN, Choudhury BB, Rao SKM, Naik B (eds) Applications of robotics in industry using advanced mechanisms. Springer International Publishing, Cham, pp 187–202
24. Nisioti A, Loukas G, Laszka A, Panaousis E (2021) Data-driven decision support for optimizing cyber forensic investigations. IEEE Trans Inform Forensic Secur 16:2397–2412. https://doi.org/10.1109/TIFS.2021.3054966
25. Paul JA, Zhang M (2021) Decision support model for cybersecurity risk planning: a two-stage stochastic programming framework featuring firms, government, and attacker. Eur J Oper Res 291:349–364. https://doi.org/10.1016/j.ejor.2020.09.013
26. Sawik T (2013) Selection of optimal countermeasure portfolio in IT security planning. Decis Support Syst 55:156–164. https://doi.org/10.1016/j.dss.2013.01.001
27. Sawik T (2020) A linear model for optimal cybersecurity investment in industry 4.0 supply chains. Int J Prod Res:1–18. https://doi.org/10.1080/00207543.2020.1856442
28. Shah A, Ganesan R, Jajodia S, Cam H (2019) Optimal assignment of sensors to analysts in a cybersecurity operations center. IEEE Syst J 13:1060–1071. https://doi.org/10.1109/JSYST.2018.2809506
29. Shah A, Ganesan R, Jajodia S, Cam H (2020) An outsourcing model for alert analysis in a cybersecurity operations center. ACM Trans Web 14:1–22. https://doi.org/10.1145/3372498
30. Stergiopoulos G, Dedousis P, Gritzalis D (2020) Automatic network restructuring and risk mitigation through business process asset dependency analysis. Comput Secur 96:101869. https://doi.org/10.1016/j.cose.2020.101869
31. Tayal K, Ravi V (2015) Fuzzy association rule mining using binary particle swarm optimization: application to cyber fraud analytics. In: 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). IEEE, Madurai, pp 1–5
32. Thakkar A, Lohiya R (2021) A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artif Intell Rev. https://doi.org/10.1007/s10462-021-10037-9
33. Won J, Bertino E (2016) Inside attack filtering for robust sensor localization. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, Xi'an, pp 931–936
34. Yamany W, Moustafa N, Turnbull B (2020) A tri-level programming framework for modelling attacks and defences in cyber-physical systems. In: Gallagher M, Moustafa N, Lakshika E (eds) AI 2020: advances in artificial intelligence. Springer International Publishing, Cham, pp 94–109
35. Zheng K, Albert LA (2019) A robust approach for mitigating risks in cyber supply chains. Risk Anal 39:2076–2092. https://doi.org/10.1111/risa.13269
36. Zheng K, Albert LA, Luedtke JR, Towle E (2019) A budgeted maximum multiple coverage model for cybersecurity planning and management. IISE Trans 51:1303–1317. https://doi.org/10.1080/24725854.2019.1584832