AISGA: Multi-objective parameters optimization for countermeasures selection through genetic algorithm

PANTALEONE NESPOLI, Department of Information and Communications Engineering, University of Murcia, Spain

FÉLIX GÓMEZ MÁRMOL, Department of Information and Communications Engineering, University of Murcia, Spain

GEORGIOS KAMBOURAKIS, European Commission, Joint Research Centre (JRC), Italy

Cyberattacks targeting modern network infrastructures are increasing in number and impact. This growing phenomenon emphasizes the central role of cybersecurity and, in particular, the reaction against ongoing threats targeting assets within the protected system. Such centrality is reflected in the literature, where several works have been presented to propose full-fledged reaction methodologies to tackle offensive incidents' consequences. In this direction, the work in [18] developed an immuno-based response approach based on the application of the Artificial Immune System (AIS) methodology. That is, the AIS-powered reaction is able to calculate the optimal set of atomic countermeasure to enforce on the asset within the monitored system, minimizing the risk to which those are exposed in a more than adequate time. To further contribute to this line, the paper at hand presents AISGA, a multi-objective approach that leverages the capabilities of a Genetic Algorithm (GA) to optimize the selection of the input parameters of the AIS methodology. Specifically, AISGA selects the optimal ranges of inputs that balance the tradeoff between minimizing the global risk and the execution time of the methodology. Additionally, by flooding the AIS-powered reaction with a wide range of possible inputs, AISGA intends to demonstrate the robustness of such a model. Exhaustive experiments are executed to precisely compute the optimal ranges of parameters, demonstrating that the proposed multi-objective optimization prefers a fast-but-effective reaction.

Additional Key Words and Phrases: Countermeasures selection, Cyberattacks countermeasures, Reaction framework, Parameters optimization, Genetic algorithm

ACM Reference Format:
Pantaleone Nespoli, Félix Gómez Mármol, and Georgios Kambourakis. 2021. AISGA: Multi-objective parameters optimization for countermeasures selection through genetic algorithm. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3465481.3470074

1 INTRODUCTION

With the significant expansion of the Information and Communication Technology (ICT) systems, network infrastructures are growing in size and complexity [4]. In this sense, their importance in modern lives is unquestionable since humans rely on the offered services every day more [9]. Such an explosion is also reflected in the adoption of powerful technologies (e.g., Blockchain [2]) and paradigms (e.g., Internet of Things (IoT) [20]), which are able to generate a great economic impact.

Nonetheless, the digital revolution carries negative consequences, too. In fact, malicious entities are continuously targeting those essential infrastructures to undermine the availability of the services and the confidentiality and integrity

Manuscript submitted to ACM

of the managed information [3]. Consequently, the quantity and disruption of cyberattacks are constantly increasing, alarming security teams worldwide struggling to find efficient measures to protect the cyberspace [8].

In such a frightening situation, one could easily say that selecting the optimal combination of countermeasures to react against cyber threats is of primary importance [5, 14]. In particular, the reactive steps need to balance the inherent tradeoff between the effectiveness of the response (i.e., the ability to block the intrusion) and the potential negative consequences (i.e., the impact on the assets of the system and the cost of those measures) [10, 27].

Besides, the reaction ecosystem still poses some unresolved challenges, forcing both academia and industry to propose novel solutions in this endless, multifaceted battle [19]. Recently, authors in [18] proposed a countermeasures selection methodology based on the application of AIS, a bio-inspired technique that mimics the behavior of the vertebrate immunological system. Such a reaction was able to minimize the risk to which the assets of the system were exposed in a more than acceptable time frame. Additionally, the authors proposed a context-aware stop condition for the AIS-powered reaction, which was calculated on-the-fly based on the measured risk value for each asset. However, the input parameters used to fire the methodology, including the number of iterations, countermeasures, and others, were chosen based on the authors' assumptions and experimental results. In this direction, one could argue that the employment of an optimization technique would be advantageous to pinpoint accurate values for those parameters, enhancing both the protection and timing performance of the proposed methodology [15].

To this extent, the paper at hand introduces AISGA, an evolutive methodology to select the input parameters of the AIS-powered reaction. Specifically, the optimizer leverages the capabilities of a GA, which permits finding optimal solutions for the input parameters through the crossover and mutation phases of the individuals. Indeed, the GA has been proved successful in solving several optimization problems in different knowledge areas, including mathematics, informatics, etc. [6]. In this sense, the presented GA methodology performs a multi-objective optimization of the parameters, i.e., risk and execution time of the AIS-powered reaction. By doing so, the GA parameters optimization allows one to thoroughly study the performance and the robustness of the AIS-powered reactions against a wide range of possible input constraints.

The remainder of the paper is organized as follows. Section 2 presents a set of relevant academic works in this area. In Section 3, the AIS-powered reaction methodology is reviewed, with a particular focus on the limitation of the input parameters computation. Then, Section 4 proposes the multi-objective parameters optimization scheme applied to the AIS reaction through the genetic algorithm. Next, Section 5 presents the outcomes of the conducted experiments. In Section 6, interesting arguments concerning the proposed procedure are discussed. Finally, Section 7 concludes the paper, proposing potential future works to contribute to the reaction ecosystem.

2 RELATED WORKS

Within the cybersecurity ecosystem, the reaction phase still poses several challenges that both academia and industry are struggling to solve [19]. To this extent, diverse works have been presented to propose effective and robust solutions to trigger against the occurrence of offensive incidents.

In [24], the authors proposed a novel risk assessment methodology based on the application of Attack Graph (AG). Such an approach enhances the standard AG-based model, avoiding frequent regenerations of the attack representation. Also, a heuristic approach is suggested to compute the optimal countermeasure to deploy that minimize the overall risk with specific budget constraints. The evaluation of the proposal was conducted in a typical organizational ICT network, demonstrating that it is cost-efficient.

Moreover, a new Autonomous Response Controller (ARC) to react against cyberattacks targeting Cyber–Physical Power Systems (CPPS) is presented in [12]. Specifically, ARC leverages the capabilities of a Hierarchical Risk Correlation Tree (HRCT), which can quantitatively measure the risk within the monitored system. This risk level is then provided to the ARC that can autonomously assess the security improvement derived by the application of certain remediations. Besides, ARC covers the uncertainty of the Intrusion Detection System (IDS) alerts by using the Competitive Markov Decision Processes (CMDPs). The capacities of the framework are demonstrated in a real substation in the CPPS with an acceptable response time.

On the line of Cyber–Physical System (CPS) protection, authors in [11] proposed a method to identify the security control to protect large-scale CPSs. By leveraging a model to calculate and aggregate the risk among the different components of CPSs, the authors used an ad-hoc version of GA to cherry-pick the adequate remediations that minimize the risk at the lowest cost. Later, a real case scenario on Cyber-Enabled Ship (C-ES) was employed to show the approach's applicability.

Furthermore, authors in [26] proposed a methodology to determine which security investments should be implemented by organizations in various risk treatment options. Those investments are connected with specific security controls, generating a model which later is solved as an optimization problem (based on the knapsack technique) using dynamic programming.

Additionally, research on decision-making issues regarding cybersecurity plans by governments and firms is offered in [22]. Bearing in mind the budget limitations, the authors suggested a methodology to compute optimal decisions on the countermeasures portfolio via a two-stage stochastic programming approach, separating prevention-detection and reaction stages. To this extent, real case studies are submitted to elaborate and discuss the approach.

Recently, an interesting methodology to select the optimal set of countermeasures to fire against the appearance of cyber threats is proposed in [18]. Such a methodology is based on the application of AIS and will be detailed in Section 3. The analyzed proposals represent crucial contributions to the reaction ecosystem. Nonetheless, the robustness of the presented methodologies against a wide range of inputs is often neglected. In this direction, the work in [18] suggested a context-aware stop condition based on experimental outcomes and authors' subjective beliefs. One could argue that an optimization approach would be beneficial to further demonstrate the capabilities of the proposed framework and discuss the main advantages and potential drawbacks.

3 AIS-POWERED REACTION

To contribute to the reaction ecosystem, the authors in [18] presented the AIS-powered reaction, an adaptation of the AIS methodology to select the optimal set of countermeasures to counteract cyberthreats happening within the monitored system. The countermeasure objects are encapsulated in a standard representation, which boosts the interoperability and sharing of the reaction-related knowledge [17]. In particular, the authors performed an initial modeling phase to translate the immuno-related concepts to the cybersecurity context. In this direction, the collection of assets $A_x \in A$ is the primary focus of the reaction procedure. At any time, those assets need to be protected against possible threats $\tau_k \in T$, namely, vulnerabilities or attacks, by minimizing the risk to which they are exposed. To this extent, the threats T represent the *antigens* against which the AIS-powered reaction computes the optimal response using *antibodies*, i.e., the set of countermeasures CM.

To select which of those atomic countermeasures $cm_i \in CM$ will be included in the optimal solution, the authors proposed the countermeasure benefit $B(cm_i) \in [1, 10]$. This index evaluates the advantage of implementing specific a remediation over a particular asset by balancing the inherent tradeoff between its effectiveness and its negative impact

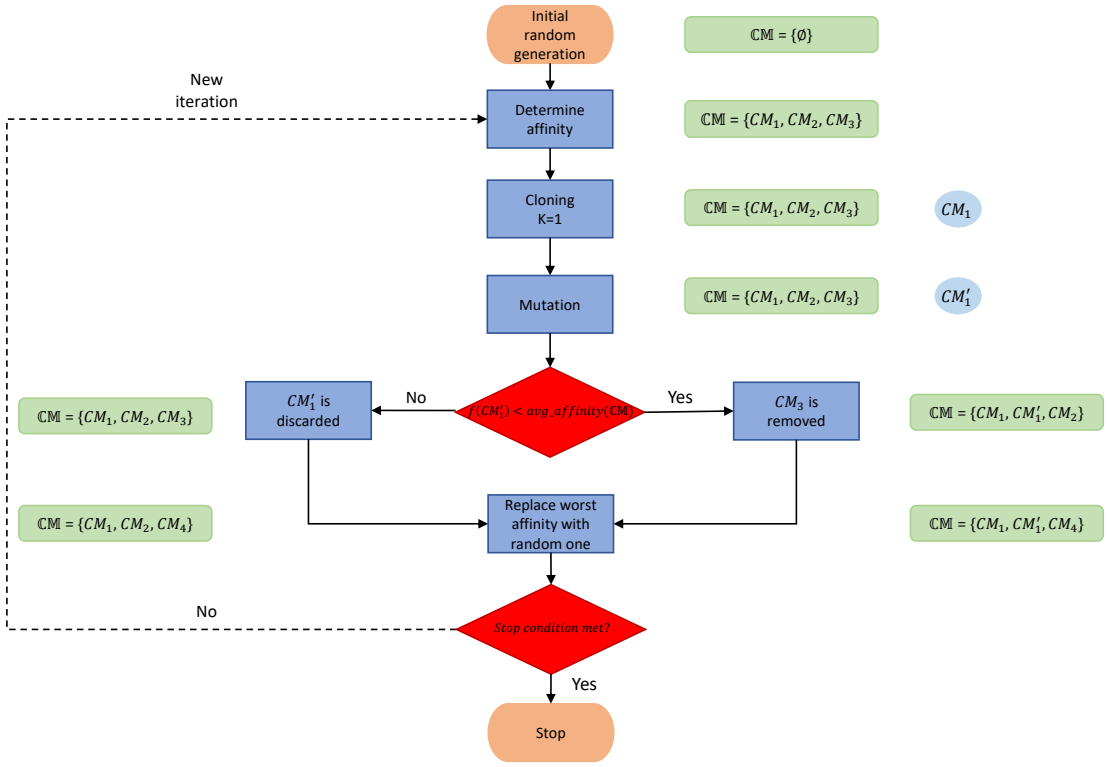

Fig. 1. AIS-powered reaction steps

and cost, as reported in Equation 1. Since the values $Effectiveness, Impact, Cost \in [0, 1]$, ω is used to shift the value to reside in the interval $[1, 10]$. In this regard, the computation of the countermeasure benefit is generalized to the enforcement of a set of countermeasures, $B(CM) \in [1, 10]$, since one or more remediations can be applied on the same asset simultaneously.

$$B(cm_i) = \omega \times (Eff(cm_i))^{1-\left(\frac{Imp(cm_i)+Cost(cm_i)}{2}\right)} \tag{1}$$

Once the concepts of the AIS have been transferred to the reaction ecosystem, the authors proposed to apply the AIS-powered reaction to minimize the difference between the risk to which the assets are exposed (i.e., the measured risk $RL(\tau_k, A_x, CM_j(A_x)) \in [0, 10]$) and the acceptable risk level assigned to each asset $\widetilde{RL}(A_x) \in [0, 10]$ by applying a set of countermeasures $CM_j(A_x)$, as shown in Equation 2. Particularly, function f is referred to as *fitness function*. The main reason behind this choice lies in the fact that the enforcement of countermeasures must elude blind risk minimization, thus avoiding both overprotection or underprotection of all the assets.

$$\min_{CM_j(A_X)} f = |RL(\tau_k, A_x, CM_j(A_x)) - \widetilde{RL}(A_x)| \tag{2}$$

It is worth remarking that, since the value of the fitness function pertains to the interval $[0, 10]$, Equation 2 means that a lower value of fitness entails a better solution.

The flow of events that characterizes the AIS-powered reaction can be summarized as follows. Depending on the type of reaction (i.e., static or dynamic), a security event is generated by the monitors deployed within the protected system (i.e., vulnerabilities scanners and IDSs) and, consequently, sent to the Security Information and Event Management (SIEM) server. Here, the events are centrally recollected, and crucial information is extracted (e.g., the involved assets, the affected vulnerabilities, etc.) to calculate the assets' current risk level. At this point, the AIS-powered reaction procedure is initiated, computing an initial random solution, i.e., a set of antibodies. Each antibody is modeled as a set of atomic countermeasures that may be implemented on the asset exposing a certain risk. Once the initial generation has been completed, the following steps are executing cyclically:

- **Determine affinity**: the affinity of each antibody belonging to the solution space is computed. That is, the benefit derived from the enforcement of the atomic countermeasures is calculated, and, consequently, the fitness is determined for each of the antibodies, and the average fitness is stored.
- **Clone antibodies**: the antibody with the best affinity (those which minimize the fitness function) are cloned. The number of generated clones depends on the mutation parameter $K \in \mathbb{N}$.
- **Mutate attributes**: each of the cloned antibodies experiences a mutation phase, where its atomic countermeasures are added/removed/modified randomly. If the affinity of the mutated clone is above the average, it is included in the solution space replacing the lowest affinity antibody. Otherwise, it is discarded.
- **Replace antibodies**: the K lowest affinity antibodies are eliminated from the solution space. In their place, K random generated antibodies are inserted, and the procedure is ready to start over again.

A graphical representation of the procedure is shown in Figure 1. Once the initial generation of the antibodies has been completed, e.g., $\mathbb{CM} = \{CM_1, CM_2, CM_3\}$, their affinity is calculated. Then, assuming that the cloning parameter $K = 1$, the best affinity antibody is cloned (in the example, CM_1). Later, CM_1 is mutated, generating CM_1'. Suppose its affinity is still better than the average affinity of the entire antibody set. In that case, CM_1' becomes part of the solution space $\mathbb{CM}$, while the worst affinity antibody, say, CM_3, is removed. Instead, if the affinity is worse than the average, CM_1' is discarded, and CM_3 remains in the solution space. Finally, the worst remaining antibody within $\mathbb{CM}$, say, CM_3 or CM_2 in this example, is removed, and a new randomly generated one replaced it, say, CM_4. At this point, if the stop condition is met, the AIS-powered methodology stops, otherwise another iteration starts.

Moreover, the authors demonstrated the applicability of the proposed approach through numerous experiments. The parameters of the underlying scenarios (i.e., threats, assets, and countermeasures) were randomly generated to better argue the capabilities of the methodology by introducing randomness. Indeed, the performances of the AIS-powered reaction are more than satisfactory both in terms of fitness and execution time. During the experimental sessions, authors vary the number of iteration of the algorithm $Iter \in [100, 1{,}000]$, the number of atomic countermeasures of the system $|CM| \in [100, 1{,}000]$, and the number of antibodies composing the solution space $|\mathbb{CM}| \in [10, 40]$, while maintaining the cloning factor $K = |\mathbb{CM}|/3$. Based on the experiments, a context-aware stop condition was also proposed, which, based on the witnessed initial fitness, assigns specific values to the abovementioned parameters $P_i \in \{Iter, |CM|, |\mathbb{CM}|\}$ following Equation 3:

$$P_i = min_i + (max_i - min_i) \times (1 - f/10) \tag{3}$$

In particular, for each parameter, min-max intervals have been determined as reported in Equation 4:

$$\begin{aligned} Iter &\in [100, 975] \\ |CM| &\in [100, 1100] \\ |\mathbb{CM}| &\in [10, 35] \end{aligned} \tag{4}$$

By capitalizing on this approach, the AIS-powered methodology calculates solutions quickly when the initial fitness is high (i.e., the assets are exposed to a high-risk situation), while computes longer searching for better solutions when the initial fitness is low. Nevertheless, the min-max intervals of the input parameters have been assigned based on the experiments' outcomes and authors' subjective beliefs. At this point, one could easily argue that a procedure to stabilize those values represents a significant step ahead to prove the performance and robustness of the AIS reaction.

4 AISGA MULTI-OBJECTIVE OPTIMIZATION

Throughout this Section, the multi-objective parameters optimization for the AIS-powered reaction is presented. In particular, AISGA leverages the capabilities of a GA to optimize the input parameters focusing on two outputs, namely, the fitness and the execution time of the solution.

Selecting the optimal parameters for combinatorial problems or machine learning tasks is challenging. In this regard, GA is a random-based classical evolutionary algorithm successfully applied to solve several computational problems in different knowledge fields [25]. Indeed, the GA applies random changes to the current solutions to generate new ones, aiming to further explore the search space [7]. More specifically, such a methodology is based on Darwin's Theory of evolution, in which a gradual process of progression leads to individuals with few changes in the population who are better adapted to their environment. In this regard, each solution within the population of a GA is also referred to as *individual*, which possesses a fitness value. Such a value is fundamental to correctly select the best individuals within the population.

GAs are generally composed of the following sequential steps, which are repeated until a predetermined stop condition is met [21]:

- **Initial population creation**: an initial population of fixed size is generated, often based on the fitness value of each individual.
- **Individuals selection**: a subset of the individuals within the population is selected to proceed to the subsequent phases. In this case, higher quality individuals have more chances of being selected.
- **Individuals crossover**: this operation recombines the genetic materials of the selected individuals to generate new offsprings. Similar to reproduction in biology, the offspring will own both parents' genes after the crossover.
- **Individuals mutation**: for each of the generated offsprings, some genes are randomly selected and mutated (their values are changed).
- **Population replacement**: a subset of the lately generated individuals (i.e., offsprings) will replace the old generation individuals. The fitness value also guides this step, aiming at improving the population with high-fitness individuals.

In our case, the GA is used to optimize the selection of the input parameters of the AIS-powered reaction. Concretely, the main goal of AISGA is to find the optimal min-max ranges of values for the parameters $P_i \in \{Iter, |CM|, |\mathbb{CM}|, K\}$ for the multi-objective fitness function g described in Equation 5. It is worth noticing that, to equalize the size of the two output parameters ($f(CM_i)$ and T), the $log_{10}X$ operator is applied to the execution time $T \in \mathbb{R}$. By doing so, the GA procedure can select the parameters with more equity.

$$min\ g = f(CM_i) + \log_{10} T \tag{5}$$

The multi-objective fitness function g in Equation 5 is charged with a dual-fold responsibility. On the one hand, the best antibody CM_i selected by the AIS methodology must minimize the fitness function f, i.e., minimize the difference between the risk to which the system's assets are currently exposed and the acceptable risk level for each asset. On the other hand, the execution time T of the AIS algorithm must be as low as possible since the timing is also an essential factor in the battle against intrusive incidents. So, by combining the fitness f and the execution time T, AISGA aims at exploring the solution space to find individuals (i.e., the input parameters to optimize) that feature both outstanding security and timing performance.

The description and possible values of the parameters of the AIS-powered reaction are reported in Table 1. In particular, Table 1 distinguishes between input parameters (the ones that the GA approach intends to optimize) and the output parameters (the ones that constitute the fitness function g). To this extent, the range of the input parameters is intentionally quite wide since, in our idea, the GA should try as many combinations of inputs as possible during its execution. Note that the other inputs requested by the AIS methodology, namely, threats, countermeasures values, assets, are randomly generated throughout the experiments.

Table 1. Description and values for each parameter to optimize of the AIS-powered reaction.

Type	Parameter	Description	Value	Domain
Input	$\|CM\|$	Number of atomic countermeasures	$[20, 2000]$	$\mathbb{N}$
	$\|\mathbb{CM}\|$	Number of antibodies	$[1, 100]$	$\mathbb{N}$
	K	Number of clones	$[1, 30]$	$\mathbb{N}$
	$Iter$	Number of iterations	$[1, 2000]$	$\mathbb{N}$
Output	$f(CM_i)$	Fitness value of the best solution	$[0, 10]$	$\mathbb{R}$
	T	Execution time of the algorithm (in seconds)	$[0, +\infty]$	$\mathbb{R}$

Additionally, the parameters of the AISGA optimizer are summarized in Table 2. Specifically, the GA procedure has been executed with $max\_iter = 500$ to let the algorithm run for an acceptable amount of time and $pop\_size = 30$ to achieve a fast convergence. The mutation and crossover probabilities have been set, respectively, to 10% and 50%, while their type is uniform. Also, the portion of the population replaced by the individuals of the previous generation, i.e., the parents, is 30%. Notably, the version of the algorithm selected for the proposed context is Elitist GA, in which the convergence curve is always non-increasing. So, the best fitness individual is equal to the best solution of the last iteration, which can help speed up the process. Following the same reasoning, the maximum number of iterations without significant improvements has been set to 50.

5 EXPERIMENTS

Numerous thorough experiments have been carried out to optimize the AIS-powered reaction parameters through the AISGA procedure. As previously mentioned, the main goal of AISGA is to find the optimal min-max range for the input parameters $P_i \in \{Iter, |CM|, |\mathbb{CM}|, K\}$ by solving the multi-objective optimization of Equation 5.

The tests have been executed on a Toshiba Portege Z30-C laptop equipped with an Intel Core i7-6500U CPU and 16 GB of DDR4 memory, using an ad-hoc adaptation of the GA python implementation proposed here[1]. Moreover, the

[1]https://pypi.org/project/geneticalgorithm2/

Table 2. Description and values for each parameter of the AISGA optimizer.

Parameter	Description	Value
max_iter	Number of iterations of the algorithm	500
pop_size	Size of the population in each iteration	30
mut_prob	Probability of each gene of the individual to be mutated	10%
mut_type	Type of mutation	uniform by center
cross_prob	Probability of crossover	50%
cross_type	Type of crossover	uniform
par_port	Portion of parents selected in the next generation	30%
elit_ratio	Ratio of elites in the population	10%
max_iter_no_improv	Maximum number of iterations without improvements	50

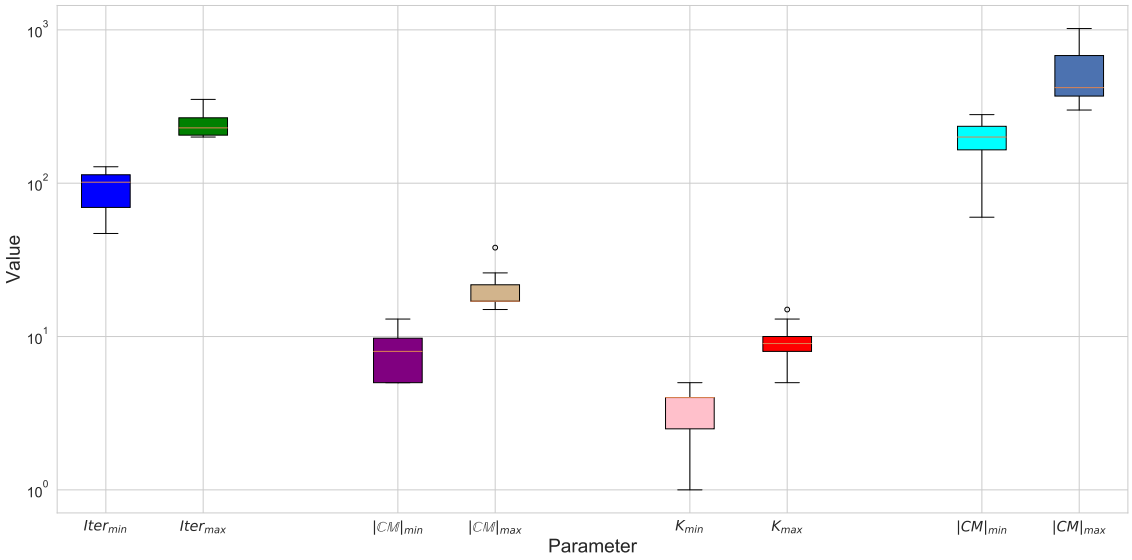

Fig. 2. Boxplot representation of the outcomes of the experiments

experiment has been repeated 100 times to prove the robustness of the approach and avoid potential outliers due to the randomness of the considered entities. Since each run of the GA lasts for 25,000 sec on average, the total duration of the experimental session was ~30 days. It is worth mentioning that the experiments have been executed simulating a small network with a number of assets $N_A = 20$ and a number of threats $|\tau| = 20$. More specifically, for each run of the AISGA procedure, 20 assets and threats are simulated, randomly generating the parameters that define such entities (i.e., the criticality of the assets together with the probability of occurrence and impact of the threats). Those values are essentially used to calculate the risk to which the assets are exposed.

The outcomes of the experiments are illustrated in Figure 2, where the parameters have been plotted on a logarithmic scale. In detail, the number of iterations $Iter$ that optimize the fitness function g is included in the interval $[102, 230]$ with regard to the median value, i.e., $Iter_{min} = 102$ and $Iter_{max} = 230$. Such a result is coherent with the outcomes in [18]. Specifically, the AIS reaction stabilizes the fitness f after ~100 iterations, and then such a value improves quite

slowly until the end of the experiment, which in that case was 1,000 iterations. In contrast, the execution time increases linearly with the number of iterations. It is clear that the number of iterations of the AIS methodology is the parameter with the highest impact on the timing performance. Hence, the multi-objective fitness-time optimization proposed by AISGA computes a low value for the maximum iteration, suggesting a fast-but-effective reaction.

Additionally, the number of antibodies $|\mathbb{CM}|$ (i.e., set of atomic countermeasures) that AIS leverages to calculate the optimal reaction is restricted to $[8, 17]$ concerning the median value, i.e., $|\mathbb{CM}|_{min} = 8$ and $|\mathbb{CM}|_{max} = 17$. Each of those antibodies contains at least one atomic remediation to counteract the 20 randomly generated threats. It has to be stressed out that, as for the iterations, a higher number of antibodies implies a longer execution time of the AIS methodology. Thus, AISGA balances the tradeoff risk-timing by maintaining a restrained quantity of antibodies.

Furthermore, the cloning factor K, designating the number of antibodies cloned during the AIS runs, belongs to the interval $[4, 9]$ regarding the median value, i.e., $K_{min} = 4$ and $K_{max} = 9$. In contrast with the work in [18] that presented a fixed value $K = |\mathbb{CM}|/3$, K is not limited to the number of antibodies in AISGA. Such a choice has been taken to give more freedom to the GA optimization when selecting the number of antibodies to clone. Obviously, the greater the value of K, the more antibodies are cloned and mutated, resulting in a broader exploration of the solution space during the AIS runs, but also in an extended execution time. Therefore, AISGA estimates that the optimal value for K is also relatively low due to the restrictions of the proposed multi-objective fitness function g.

Finally, the number of atomic countermeasures $|CM|$ used by the AIS-powered reaction to minimize the total risk is included in the interval $[200, 420]$ concerning the median value, i.e., $|CM|_{min} = 200$ and $|CM|_{max} = 420$. Since the experiments have been executed simulating a network of 20 assets on average, these results signify that each asset should be equipped with between 10 and 21 countermeasures approximately. Such an outcome further emphasizes the importance of possessing comprehensive countermeasure knowledge within the protected system to accurately counteract against potential threats. However, the number of countermeasures also impacts the timing performance of the AIS reaction since the procedure must enforce several countermeasures and, consequently, compute more benefit indexes.

All in all, the experimental outcomes can give one an interesting perspective on both the risk and timing performance of the AIS-powered reaction methodology. Recalling that the inputs of the procedure (i.e., assets, countermeasures, and threats) have been randomly simulated and that the GA optimization procedure is based on the randomicity, one can conclude that the robustness of the AIS model against a wide range of input values has been demonstrated. Besides, thanks to the AISGA optimizer, the min-max ranges of the input parameters have been computed, balancing the inherent tradeoff between minimizing the risk and execution time of the methodology simultaneously.

6 DISCUSSION

In the previous Sections, the AISGA procedure has been presented and tested, demonstrating its capabilities to select the optimal ranges of parameters to feed the AIS reaction methodology. Nonetheless, some arguments regarding the countermeasures selection ecosystem are worthy of discussion.

As widely reviewed in Section 3, the AIS-powered reaction aims to select the optimal set of atomic countermeasures to fight against cyber threats. Such a selection is intended to help security administrators in the decision-making process, guiding them towards the correct actions to eradicate the threat. Recently, the decision-making ecosystem has witnessed the rise of reinforcement learning methods, which are able to learn over time and improve their accuracy [1]. Undoubtedly, those methods look promising, featuring exciting capabilities. However, their performance directly depends on the scenario on which they are implemented, requiring an initial learning phase. On the contrary, the

combination of AIS reaction and AISGA optimization procedure can compute the optimal reaction using only the countermeasure knowledge of the system. In this sense, the proposed methodology can be defined as generic, adapting itself to different scenarios. Nevertheless, the approaches can be combined, e.g., AIS can be used to send feedback to the learning procedure to speed up the process, being supervised by the administrators at any time, thus contributing to the overall cyber threat intelligence.

Additionally, since AIS possesses a defensive focus, one could assume that potential attackers would try to undermine its capabilities through specific counterintelligence actions, i.e., adversarial tactics [23]. Specifically, an attacker could try to force several reaction steps, for example, to consume the system's resources. In this scenario, the fitness level that fires the procedure (i.e., the difference between the measured and acceptable risk for each asset) should be tuned to consider such tactics in an effort to mitigate their effect. However, the robustness of the AIS-powered response has been extensively demonstrated throughout the exhaustive experiments conducted by the AISGA optimizer. Moreover, as we will see in Section 7, an interesting future line consists of enriching the countermeasures knowledge with offensive countermeasures, which can be fired in the mentioned counterintelligence situations.

7 CONCLUSIONS AND FUTURE WORK

The galloping digitalization, cloudification, and the so-called "new norm" introduced by the pandemic are impacting our lives every day more. Humans leverage the hyperconnectivity offered by the modern ICT systems, consuming services to improve their quality of lives at an astonishing speed [13]. Nevertheless, such a revolution also implies the appearance of ill-motivated entities that perform malicious actions against those systems to achieve their spiteful objectives. Indeed, powerful cyberattacks undermine the stability of the cyberspace, claiming the attention of security teams from both public and private sectors [16].

In this direction, several proposals have been presented, aiming to develop a full-blown reaction strategy to fire against potential cyber threats. Among them, the work in [18] proposed an interesting immuno-based response approach based on the AIS methodology. In fact, the AIS-powered reaction is able to compute the optimal set of atomic countermeasures to enforce on the assets of the system, balancing the tradeoff between the effectiveness of reaction and possible negative consequences of its implementation. This procedure looks promising in the battle against offensive incidents, achieving excellent results in a more than acceptable time lapse. Nevertheless, the robustness of the methodology against a wide range of possible inputs has been neglected. Besides, the experimental inputs for certain features, including the context-aware stop condition, have been picked based on outcomes results and authors' beliefs.

Under this prism, the paper at hand proposed AISGA, a multi-objective approach that leverages the capabilities of the GA to optimize the selection of the parameters of the AIS solution. Specifically, AISGA performs risk minimization and time reduction concurrently thanks to the constant mutation and crossover phases of the selected individuals. Exhaustive experiments were executed to flood the AIS methodology with a broad series of parameters, aiming to prove both the robustness of the AIS-powered model and to explore the solution space extensively. By using the multi-objective fitness function g, the computed intervals were quite reduced, suggesting that a fast-but-effective reaction was preferred to a meticulous-but-expensive one.

Future work will explore the possibility of implementing the AIS reaction methodology in a real use-case scenario to study the impact of the optimized parameters. Additionally, the viability of enriching the countermeasures knowledge with offensive countermeasures is worth of study, considering their importance in military contexts.

ACKNOWLEDGMENTS

This work was partially supported by the University of Murcia through the FPU (Formación del Profedorado Universitario) Predoctoral Contract, in part by the MINECO (Ministerio de Economía y Empresa), Spain, through the Ramón y Cajal Research Contract, under Grant RYC-2015-18210, by the European Social Fund, and by the European Commission through 5GZORRO (Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks, grant No. 871533) and PALANTIR (Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises, grant No. 883335) projects.

REFERENCES

[1] Ahmad Hoirul Basori and Sharaf Jameel Malebary. 2020. *Deep Reinforcement Learning for Adaptive Cyber Defense and Attacker's Pattern Identification.* Springer International Publishing, Cham, 15–25. https://doi.org/10.1007/978-3-030-19353-9_2

[2] Juan Velandia Botello, Andrés Pardo Mesa, Fabián Ardila Rodríguez, Daniel Díaz-López, Pantaleone Nespoli, and Félix Gómez Mármol. 2020. BlockSIEM: Protecting Smart City Services through a Blockchain-based and Distributed SIEM. *Sensors* 20, 16 (2020), 1–21. https://doi.org/10.3390/s20164636

[3] Daniel Díaz López, María Blanco Uribe, Claudia Santiago Cely, Andrés Vega Torres, Nicolás Moreno Guataquira, Stefany Morón Castro, Pantaleone Nespoli, and Félix Gómez Mármol. 2018. Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. *Wireless Communications and Mobile Computing* 2018 (2018), 1–18. https://doi.org/10.1155/2018/3029638

[4] David Goad, Andrew T. Collins, and Uri Gal. 2021. Privacy and the Internet of Things : An experiment in discrete choice. *Information & Management* 58, 2 (2021), 103292. https://doi.org/10.1016/j.im.2020.103292

[5] Gustavo Gonzalez-Granadillo, Elena Doynikova, Joaquin Garcia-Alfaro, Igor Kotenko, and Andrey Fedorchenko. 2020. Stateful RORI-based countermeasure selection using hypergraphs. *Journal of Information Security and Applications* 54 (2020), 102541. https://doi.org/10.1016/j.jisa.2020.102541

[6] Antonio Gómez-Mompeán and Rafael Lahoz-Beltra. 2020. An Evolutionary Computing Model for the Study of Within-Host Evolution. *Computation* 8, 1 (2020), 1–23. https://doi.org/10.3390/computation8010005

[7] Khader M. Hamdia, Xiaoying Zhuang, and Timon Rabczuk. 2021. An efficient optimization approach for designing machine learning models based on genetic algorithm. *Neural Computing and Applications* 33, 6 (01 Mar 2021), 1923–1933. https://doi.org/10.1007/s00521-020-05035-x

[8] Limin Huang. 2020. Application of Artificial Intelligence Technology in Security Defense of Cyberspace. *IOP Conference Series: Materials Science and Engineering* 750 (mar 2020), 012104. https://doi.org/10.1088/1757-899x/750/1/012104

[9] Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, and Gregorio Martínez Pérez. 2019. Towards the autonomous provision of self-protection capabilities in 5G networks. *Journal of Ambient Intelligence and Humanized Computing* 10, 12 (01 Dec 2019), 4707–4720. https://doi.org/10.1007/s12652-018-0848-6

[10] Stefano Iannucci, Valeria Cardellini, Ovidiu Daniel Barba, and Ioana Banicescu. 2020. A hybrid model-free approach for the near-optimal intrusion response control of non-stationary systems. *Future Generation Computer Systems* 109 (2020), 111 – 124. https://doi.org/10.1016/j.future.2020.03.018

[11] Georgios Kavallieratos, Georgios Spathoulas, and Sokratis Katsikas. 2021. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. *Sensors* 21, 5 (2021), 1–21. https://doi.org/10.3390/s21051691

[12] Hisham A. Kholidy. 2021. Autonomous mitigation of cyber risks in the Cyber–Physical Systems. *Future Generation Computer Systems* 115 (2021), 171–187. https://doi.org/10.1016/j.future.2020.09.002

[13] Changsung Lee, Jaewook Jung, and Jong-Moon Chung. 2020. DEFT: Multipath TCP for High Speed Low Latency Communications in 5G Networks. *IEEE Transactions on Mobile Computing* (2020), 1–1. https://doi.org/10.1109/TMC.2020.3000041 Early Access.

[14] Fenghua Li, Yongjun Li, Siyuan Leng, Yunchuan Guo, Kui Geng, Zhen Wang, and Liang Fang. 2020. Dynamic countermeasures selection for multi-path attacks. *Computers & Security* 97 (2020), 101927. https://doi.org/10.1016/j.cose.2020.101927

[15] Hui Li, Xiao Liu, Zhiguo Huang, Chenbo Zeng, Peng Zou, Zhaoyi Chu, and Junkai Yi. 2020. Newly Emerging Nature-Inspired Optimization - Algorithm Review, Unified Framework, Evaluation, and Behavioural Parameter Optimization. *IEEE Access* 8 (2020), 72620–72649. https://doi.org/10.1109/ACCESS.2020.2987689

[16] Jorge Maestre Vidal, Marco Antonio Sotelo Monge, Sergio Mauricio Martínez Monterrubio, Lorena Isabel Barona López, and Ángel Leonardo Valdivieso Caraguay. 2019. Profits at the Dawn of Cybercrime-as-a-Service. In *2019 International Conference on Information Systems and Software Technologies (ICI2ST)*. IEEE, Quito, Ecuador, 71–78. https://doi.org/10.1109/ICI2ST.2019.00017

[17] Pantaleone Nespoli, Félix Gómez Mármol, and Jorge Maestre Vidal. 2021. Battling against cyberattacks: Towards pre-standardization of countermeasures. *Cluster Computing* 24 (Mar 2021), 57–81. https://doi.org/10.1007/s10586-020-03198-9

[18] Pantaleone Nespoli, Félix Gómez Mármol, and Jorge Maestre Vidal. 2021. A Bio-Inspired Reaction Against Cyberattacks: AIS-Powered Optimal Countermeasures Selection. *IEEE Access* 9 (2021), 60971–60996. https://doi.org/10.1109/ACCESS.2021.3074021

[19] Pantaleone Nespoli, Dimitrios Papamartzivanos, Félix Gómez Marmol, and Georgios Kambourakis. 2018. Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. *IEEE Communications Surveys Tutorials* 20, 2 (Secondquarter 2018), 1361–1396. https://doi.org/10.1109/COMST.2017.2781126

[20] Pantaleone Nespoli, David Useche Peláez, Daniel Díaz López, and Félix Gómez Mármol. 2019. COSMOS: Collaborative, Seamless and Adaptive Sentinel for the Internet of Things. *Sensors* 19, 7 (2019), 1–29. https://doi.org/10.3390/s19071492

[21] Dimitrios Papamartzivanos, Félix Gómez Mármol, and Georgios Kambourakis. 2018. Dendron : Genetic trees driven rule induction for network intrusion detection systems. *Future Generation Computer Systems* 79 (2018), 558–574. https://doi.org/10.1016/j.future.2017.09.056

[22] Jomon A. Paul and Minjiao Zhang. 2021. Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker. *European Journal of Operational Research* 291, 1 (2021), 349–364. https://doi.org/10.1016/j.ejor.2020.09.013

[23] Kui Ren, Tianhang Zheng, Zhan Qin, and Xue Liu. 2020. Adversarial Attacks and Defenses in Deep Learning. *Engineering* 6, 3 (2020), 346–360. https://doi.org/10.1016/j.eng.2019.12.012

[24] Orly Stan, Ron Bitton, Michal Ezrets, Moran Dadon, Masaki Inokuchi, Yoshinobu Ohta, Tomohiko Yagyu, Yuval Elovici, and Asaf Shabtai. 2021. Heuristic Approach for Countermeasure Selection Using Attack Graphs. In *2021 2021 IEEE 34th Computer Security Foundations Symposium (CSF)*. IEEE Computer Society, Los Alamitos, CA, USA, 63–78. https://doi.org/10.1109/CSF51468.2021.00003

[25] Yang Su, Saimeng Jin, Xiangping Zhang, Weifeng Shen, Mario R. Eden, and Jingzheng Ren. 2020. Stakeholder-oriented multi-objective process optimization based on an improved genetic algorithm. *Computers & Chemical Engineering* 132 (2020), 106618. https://doi.org/10.1016/j.compchemeng.2019.106618

[26] Ganbayar Uuganbayar, Artsiom Yautsiukhin, Fabio Martinelli, and Fabio Massacci. 2021. Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security* 101 (2021), 102121. https://doi.org/10.1016/j.cose.2020.102121

[27] Bingfeng Xu, Zhicheng Zhong, and Gaofeng He. 2020. A Minimum Defense Cost Calculation Method for Attack Defense Trees. *Security and Communication Networks* 2020 (2020). https://doi.org/10.1155/2020/8870734