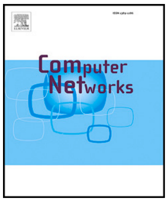
Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Novel modeling and optimization for joint Cybersecurity-vs-QoS Intrusion Detection Mechanisms in 5G networks

Arash Bozorgchenani [a,*], Charilaos C. Zarakovitis [b], Su Fong Chien [c,1], Tiew On Ting [d,1], Qiang Ni [e], Wissam Mallouli [f]

[a] *School of Computing, University of Leeds, Leeds, UK*
[b] *National Center For Scientific Research "Demokritos", Greece*
[c] *Multidisciplinary Research and Innovation Centre, MIMOS Berhad, Kuala Lumpur, Malaysia*
[d] *Stony Brook Institute at Anhui University (SBIAHU), Hefei City, Anhui Province, PR China*
[e] *School of Computing and Communications, Lancaster University, Lancaster, UK*
[f] *Montimage EURL, France*

ARTICLE INFO

Keywords:
Cybersecurity
Intrusion detection mechanisms
Optimization

ABSTRACT

The rapid emergence of 5G technology brings new cybersecurity challenges that hold significant implications for our economy, society, and environment. Among these challenges, ensuring the effectiveness of Intrusion Detection Mechanisms (IDMs) in monitoring networks and detecting 5G-related cyberattacks is of utmost importance. However, optimizing cybersecurity levels and selecting appropriate IDMs remain as critical and ongoing challenges. This work considers multiple pre-deployed distributed Security Agents (SAs) across the network, each capable of running various IDMs, where they differ by their effectiveness in detecting the attacks (referred to as security term) and the consumption of resources (referred to as Quality of Service (QoS) costs). We formulate a joint security and QoS utility function leveraging the Cobb–Douglas production utility function. There are several parameters that impact the joint objective problem, including the set of elasticity parameters, that reflect the importance of the two objectives. We derive an optimal set of elasticity parameters in closed form to identify the balancing point where both objectives have equal utility values. Through comprehensive simulations, we demonstrate that increasing the detection level of SAs enhances the security utility while simultaneously diminishing the QoS utility, as more computational, bandwidth, and monetary resources are utilized for IDM processing. After optimization, our mechanism can strike an effective balance between cybersecurity and QoS overhead while demonstrating the importance of different parameters in the joint problem.

1. Introduction

The advent of 5G has enabled various types of services, such as smart homes, Vehicle-to-Vehicle (V2V) communication, and industry 4.0, through the blending of different technologies and advances [1]. However, the evolution of security in telecommunications networks from ensuring proper billing system functionality to protecting against physical attacks and privacy concerns has resulted in increased security challenges with the introduction of 5G and beyond. These challenges stem from the larger number of users, heterogeneity of devices, new services, and the utilization of new technologies [2]. Therefore, addressing security in 5G has become crucial to maintaining the integrity of the network and preserving the user experience.

Network-based Intrusion Detection Systems (IDSs) are designed to detect and signal potential attacks or suspicious activity that could threaten the integrity, confidentiality, or availability of a network. IDSs are designed to ensure network and data security by analyzing the characteristics of the network traffic data, identifying malicious network behavior, generating alerts, and formulating reasonable defense strategies [3,4]. Security Agents (SA), enabled to execute the IDS techniques, are deployed strategically and inspect encrypted traffic and extract key features for identifying potential security breaches. Once the agents detect any suspicious activity, they alert the orchestrator, which can then take appropriate mitigation actions. Even though the terms IDSs and Intrusion Detection Mechanisms (IDMs) are interchangeably used in the literature, it is important to differentiate them since the former

[*] Corresponding author.
E-mail address: a.bozorgchenani@leeds.ac.UK (A. Bozorgchenani).
[1] Authors contributed equally.

https://doi.org/10.1016/j.comnet.2023.110051
Received 24 July 2023; Received in revised form 21 September 2023; Accepted 29 September 2023
Available online 4 October 2023

may incorporate multiple techniques (or IDMs) for detecting attacks. SAs can monitor the system at different levels of detection exploiting different IDMs, with higher levels leading to greater accuracy in identifying potential intrusions. However, monitoring the system at higher detection levels corresponds to more sophisticated IDMs, which consume more resources, including network bandwidth, computational resources, and monetary costs, resulting in an increased monitoring overhead. Ensuring a high level of Quality of Service (QoS) is crucial for preserving the 5G user experience, especially when a significant amount of data is generated in the network. However, a classic dilemma arises since high-security services provided by IDMs can often lead to decreased QoS performance due to the additional network resources required for IDM processing. [5]. Therefore, the system needs to balance the trade-off between maximizing the IDM detection performance (i.e., keeping the network secure) and minimizing the resource costs (i.e., preserving the user QoS). This brings the challenge to determine which IDM is the most efficient in a system to compromise the security and QoS objectives at different time instances. Please note that in the rest of the paper, the term QoS refers to resource consumption or monitoring overhead.

We note a large body of literature investigating the problem of intrusion detection in 5G networks, in-vehicle networks, vehicular communication, Internet of Things (IoT), and small-cells [6–10]. Moreover, there have been numerous works studying how to secure the system by providing countermeasures considering the security and QoS [11–15]. These efforts rely on either multi-objective Genetic Algorithm optimization or game-theoretic methods to provide cybersecurity remediation. However, except our previous work in [16], there is no attempt to address the problem of IDM selection problem as intended in this work.

Motivated by the above, we first study how we can incorporate security with QoS in final formulas reflecting the nature of the problem by adopting the production function theory. We formulate the joint security-vs-QoS problem for the IDM selection problem and provide analytical studies that how we can balance between the two objectives by introducing multiple parameters. The significance of such a trade-off stands paramount to realizing and optimizing the cybersecurity network because it accounts for the network's states/conditions and system preferences at different time instances toward selecting the IDMs for the SAs.

The rest of the paper is organized as follows. Section 2 lists the literature review of the most related papers and highlights our contribution. In Section 3, we describe the system model, formulate the problem, and present the optimal solution for obtaining the balancing point of the two objectives. In Section 4, we present the simulation results. Section 5 concludes the paper.

2. Related works

In this section, we first review the most relevant studies and then provide our observations of the problem and contributions.

2.1. The literature review

Intrusion detection is an integral part of network security and has become a research hotspot in recent years. A large body of works dedicated their research to the problem of IDS design for various scenarios. A taxonomy and a review of the significant research work on IDSs can be found in [17–20]. One particular study [21] introduced a framework for a network IDS that utilizes image processing techniques. Additionally, the authors in [22] developed an IDS tailored explicitly for IoT applications, leveraging the message queuing telemetry transport Protocol. These works, among many others, highlight the ongoing efforts to enhance IDS capabilities and adapt them to various domains and technologies.

Progress in the field of Machine Learning (ML) is paving the way for improving and developing intelligent and effective IDSs. To achieve a high detection rate, data normalization plays an important role in ML-based IDSs. In [23], the authors proposed a statistical method that can identify the most suitable normalization method for IoT and traditional network environments datasets that gives the highest accuracy for an IDS. Over the past few years, there has been a proliferation of efficient deep learning models like deep belief networks, deep convolutional neural networks, recurrent neural networks, and deep generative networks. These models have found application in the development of network IDSs [3,24]. [25] introduced a deep learning model using stacked non-symmetric deep auto-encoders for accurate network intrusion detection. In [26], deep convolutional neural networks and weight-dropped long short-term memory networks are combined in big data environments to improve detection accuracy. Authors in [27] developed a hybrid deep learning framework with convolutional and recurrent neural networks for predicting and classifying malicious network attacks. [28] proposed a model that combines a convolutional neural network and a gated recurrent unit to address accuracy and class imbalance issues in intrusion detection. [29] implemented an IDS using different recurrent neural networks. As for privacy reasons many users opt not to share their device-generated dataset with other devices. For this reason, the authors in [30] propose a Federated Learning-based approach for IoT intrusion detection problems. The imbalance between the attack and normal traffic has motivated the authors in [31] to propose an IDS called pretraining Wasserstein generative adversarial network.

Studies have shown that running an IDS in a mobile device is energy and time-consuming and takes memory capacity. In [32] the authors propose a vehicular-edge computing fog-enabled approach enabling offloading intrusion detection tasks to federated vehicle nodes to be cooperatively executed with minimal latency.

There are also several papers studying IDS evaluation. [33] presents a framework for the evaluation of IDSs. The framework studies the advantages and disadvantages of multiple evaluation criteria, including the Bayesian detection rate, the expected cost, and the sensitivity. The authors in [34] present an IDM and a performance reliability evaluation model that analyzes the performance and hardware dependability of IDMs. The proposed evaluation model considers imbalanced sample ratios and provides a comparative analysis of IDMs.

There are also many papers studying feature selection to improve the performance of IDSs. [35] proposed an approach for generating optimized ensemble IDS by employing feature selection techniques. Six feature selection methods are compared, and the selected features are used in combination with different classification algorithms to create ensemble IDSs. [36] presents an IDS that utilizes feature selection and clustering algorithms based on filter and wrapper methods. The filter method employed is the feature grouping based on the linear correlation coefficient algorithm, while the wrapper method utilized is the cuttlefish algorithm. The proposed method employs a decision tree classifier. [37] proposes two models for intrusion detection and classification in secure networks. The first one reduces feature dimensionality using a novel algorithm and incorporates trust relationships between nodes. The second one introduces dynamic node cleansing and restricts exposure time. Both models utilize ML and past node behavior for classification. In [38] the authors propose a detection model based on normalized mutual antibodies information feature selection and adaptive quantum artificial immune. In a similar work in [39], the authors propose a detection model using normalized mutual information feature selection and cooperative evolution of multiple operators based on an adaptive parallel quantum genetic algorithm.

While there have been numerous papers focusing on designing IDSs, conducting feature selection on IDMs, and evaluating IDSs, there remains a notable gap in the research regarding the selection of IDMs for a specific system or operator. Specifically, the task of selecting the most suitable IDM at any given time requires considering the detection efficiency of each IDM and the associated costs in terms of QoS impact. In our previous work in [16], we made progress in addressing this issue.

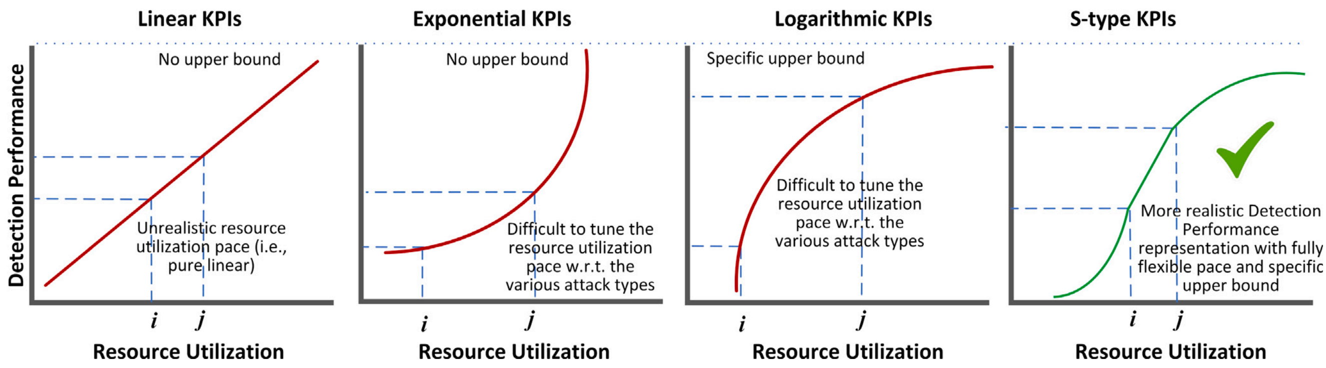


Fig. 1. Indicative comparison between existing works on cybersecurity function modeling.

However, our current work distinguishes itself from [16] in several key aspects. First and foremost, we provide a more detailed formulation for the security and QoS utility function. Unlike the previous work which demonstrated a linear relationship between the two objectives, we introduce a non-linear function leveraging the Cobb–Douglas production utility function. This enhanced formulation captures the intricate dynamics between security and QoS more accurately. Moreover, we exploit estimated values obtained from a 5G monitoring tool in the simulation results. This enables us to incorporate realistic data into our analysis and further enhance the validity and relevance of our findings. Furthermore, our current study includes analytical studies that allow us to derive the balancing point between the two objectives in closed form. This analytical approach provides valuable insights and facilitates a deeper understanding of the trade-offs between cybersecurity and QoS.

2.2. Our observations and contributions

We have observed a lack of relevant studies that have attempted to elucidate the impact of system costs or monitoring resource utilization on detection performance. System monitoring entails the consumption of resources and effort, such as CPU utilization, bandwidth usage, and monetary expenses, among others. Moreover, different IDMs operate in distinct manners and require varying resources. Thus, it is crucial to incorporate this relationship into the final formulas.

Several potential Key Performance Indicators (KPIs) can be defined to illustrate this correlation, including (1) linear KPI functions, (2) exponential KPI functions, and (3) logarithmic KPI functions. However, we argue that such cases fail to adequately capture the true nature of the problem due to the following reasons. Using linear functions does not accurately represent the relationship between resource utilization and detection performance for different types of attacks. It assumes an equal and fixed increase or decrease in detection pace with each resource allocated, regardless of the attack type. This oversimplification does not capture the varying complexities associated with different attack types. Although exponential functions can demonstrate a rapid increase or decrease in detection performance with resource utilization, they fail to incorporate an upper bound for the process. Additionally, they do not adapt the pace of the graph with respect to resource utilization, thereby, overlooking the need for flexibility in optimizing resource allocation. Logarithmic functions come closer to describing the phenomenon by providing an upper bound and flexibility in the pace of detection performance with resource utilization. However, they still lack the necessary degrees of freedom to adjust the pace over resource utilization for all types of attacks. Different attack types may require different levels of resource allocation to achieve optimal detection performance. Therefore, while linear, exponential, and logarithmic KPI functions have their merits, they do not adequately capture the intricacies and varying complexities associated with different types of attacks and the corresponding resource utilization in IDSs. A more nuanced approach is required to accurately model and optimize the detection performance in relation to resource utilization.

We define detection performance by considering the above KPIs in relation to changes in resource utilization, while also accounting for the varying complexities associated with detecting different types of attacks. To illustrate this concept, we classify attacks into three primary categories:

1. Category 1: These attacks are relatively easy to detect since their detection relies on known signatures or patterns in the packets, e.g., poisoning attacks with malformed packets. With limited resources, we can effectively detect these attacks, which constitute the majority of the incidents detected. The detection performance for these attacks exhibits more exponential behavior, indicating that with each additional resource allocated, the detection capability significantly improves.
2. Category 2: These attacks may involve correlating at least two or three events to identify them. Examples of these attacks include multi-faced attacks or Advanced Persistent Attacks. The complexity of detection for these attacks is moderate. By allocating additional resources, we can improve our ability to detect attacks falling into this category in a linear manner.
3. Category 3: These attacks are highly complex to detect and necessitate advanced techniques such as statistical analysis and ML techniques, e.g., low Distributed Denial of Service attacks. These attacks are less common than those in Categories 1 and 2. To effectively detect new attacks within Category 3, a significant allocation of resources is required, given their complexity and rarity. The detection performance of these attacks exhibits logarithmic behavior.

In light of the above considerations, we conceptualize the detection performance of IDSs with respect to resource utilization as a multi-dimensional space, which can be characterized by the properties of an S-Type function. In this context, the problem can be described as having an explicit configurable upper bound, as well as a configurable rate of increase or decrease in relation to the utilization of resources and efforts. Fig. 1 exhibits the three KPI functions along with our proposed KPI function that combines these three functions to account for the complexities associated with detecting different attack types. The incorporation of these functions results in an S-shaped curve, offering a greater range of flexibility to accurately model various threat types and their severity. This S-shaped curve allows for a more comprehensive representation of the detection performance and resource utilization relationship.

This is a significant research finding that has not yet been provided previously, to our knowledge, which can be approached based on well-known Theorems coming from the Production Function Theory called Cobb–Douglas functions, which have been used extensively in Finance Sciences [40]. Adopting Production Function Theory and Utility Theory, we can blend performance dynamics related to QoS and security within the S-Type Cybersecurity function, to finally produce a multi-performance KPI toward balancing all these performances jointly.

This work introduces, for the first time, the means to approach the IDM selection problem explicitly based on specific standard Theorems, thereby opening new ways for existing and future studies to extend their findings over mathematically precise Cybersecurity solutions for system automation, optimization, and management. Our contributions are summarized in the following:

1. Design of a new utility function to correlate security with the QoS of the network for the IDM selection problem by adopting the Cobb–Douglas production function, which, to our knowledge, has not been attempted by relevant studies;
2. Formulation of the IDM selection problem as an optimization problem considering the security and QoS constraints, which is unique on its kind;
3. Derivation of optimal elasticity parameters, which correlate the importance of security and QoS, allowing to finding the balancing point between the two objectives;
4. Demonstration via simulations to showcase the performance of the system under various preference settings.

3. System model and problem formulation

Let us consider a heterogeneous architecture, comprising IoT devices, base stations, servers, and various core-level network functions, all of which are susceptible to cyberattacks. To ensure the security of the network, we have deployed some SAs in the network to monitor the system. Each SA can perform system monitoring with a specific security detection level. Each of these security detection levels enables the SA to identify certain attack types in the system. For instance, one security level may be used for signature-based intrusion detection, while another may be used for anomaly-based intrusion detection and another one for complex event processing or hybrid intrusion detection methods. Higher detection levels increase the efficiency and accuracy of the SA in detecting attack types but at a higher system cost. Therefore, there is a trade-off to consider in selecting the security detection level for each SA, which is the focus of this paper. Please note that in the rest of the paper, we might refer IDMs as security detection levels.

Let us define the set of M SAs with $\mathcal{A} = \{a_1, \dots, a_m, \dots a_M\}$. We denote the security detection level of a SA as L_m which equals n, where $n \in \{1, \dots, N\}$, representing different detection levels. The problem involves determining the appropriate detection level to assign to each SA to detect attacks in the system effectively while maximizing the system utility function. The system utility function is composed of security, Y_m^{Sec} and QoS, Y_m^{QoS} utility functions.

To evaluate the efficiency of a security detection level, we measure the number of attacks the SA can detect out of the total number of known attacks by incorporating the possibility of the existence of unknown attacks in the system similar to [16]. Let us define H, H', and $\bar{H}$ as the number of detected attacks based on the selected detection level, the total number of known attacks, and the number of unknown attacks.[2] The number of unknown attacks is also a portion of the known attacks, i.e., $\bar{H} \in [0 \quad \%\imath] \times H'$. We define the efficiency of detection at a specific level as $\rho_m(L_m) = \left(\frac{H(L_m)}{H'+\bar{H}}\right)$, where $H(L_m) = \zeta(L_m) \times H'$ and $\zeta(L_m)$ is the $\%$ of detected cyberattacks at a detection level. By incorporating the impact of the number of detected attacks with the efficiency of a security detection level, we define the security utility function of the security level L_m of SA m as

$$Y_m^{\text{Sec}}(L_m) = \rho(L_m) \times H(L_m) \tag{1}$$

On the other hand, achieving high security detection accuracy requires a system to allocate resources to enable this functionality for the SAs. The cost associated with deploying a specific SA within the network is not solely determined by the number of SAs but also by the inclusion of IDMs, categorized in our paper as Levels 1 to 3. Each of these levels exhibits unique resource consumption profiles, and this variance in resource utilization directly impacts the overall cost of SA deployment. In our model, we consider that different IDMs running on SAs consume different network bandwidth and computational resources and they also incur some monetary costs for performing the system monitoring. In order to model bandwidth, computational resources, and monetary costs we rely on the observations made on our monitoring tools during experimentation. More precisely, let us suppose that the system is initially purified from threats and at time instance T_1 a single attack A is detected, for which, the system consumes ϑ computational resources (RAM, CPU, HDD, etc. for implementing the necessary security process for threat monitoring), which has an impact on the overall system bandwidth, i.e., the ϑ computational resources impose a b system overhead. Supposing that we detect a second threat at the second time instance T_2, the computational resources, and bandwidth do not increase linearly, but logarithmically, i.e., for 2 threats, the system does not consume $2 \times \vartheta$ and $2 \times b$, but slightly fewer resources. Hence, we define bandwidth, $B(L_m)$, and computational consumption, $\eta(L_m)$, for the detection level L_m as

$$B(L_m) = \log\Big(1 + H(L_m) \times b\Big) \tag{2}$$

$$\eta(L_m) = \log\Big(1 + H(L_m) \times \vartheta\Big) \tag{3}$$

On the other hand, monetary costs include both fixed and variable prices. Let us assume the detection process costs c_1 fixed and c_2 variable monetary resources to the operator. The first part can be the system costs and the second part the marginal costs. We assume upon detection of a second attack, the fixed part increases linearly, while the variable part logarithmically. Hence, we define the monetary costs as

$$\Psi(L_m) = H(L_m) \times c_1(L_m) + \log\Big(1 + H(L_m) \times c_2(L_m)\Big) \tag{4}$$

where c_1 and c_2 represent the fixed and variable monetary costs for the given detection level, respectively. Hence, the overall QoS Utility function for a specific security level can be defined as

$$Y_m^{\text{QoS}} = B(L_m) + \eta(L_m) + \Psi(L_m) \tag{5}$$

In our model, we assume that the bandwidth, computational resources, and monetary costs are shared among the M SAs because SAs are deployed as containers/pods over physical servers and the allocated resources are virtualized. As the graph of the attack detection exhibits an S-shaped behavior w.r.t. attack types and utilized resources, we adopt the Cobb–Douglas production function to define our joint multi-objective problem. The Cobb–Douglas utility function is defined as

$$Q(K, L) = AK^{\alpha}L^{\beta} \tag{6}$$

where A, K and L represent the total factor productivity, Capital, and Labor inputs, and α and β are the output elasticities of capital and labor where $\alpha + \beta = 1$. Let us map K and L to security and QoS utilities and write the joint security and QoS function using the Cobb–Douglas function as

$$Q(Y_m^{\text{Sec}}, Y_m^{\text{QoS}}) = A\left(Y_m^{\text{Sec}}\right)^{\alpha} \times \left(\frac{\nu}{Y_m^{\text{QoS}}}\right)^{\beta} \tag{7}$$

The above equation represents that the Security is the Capital and the QoS is the labor required to achieve that Capital. Please note that the QoS term, as stated earlier, is the system costs/monitoring overhead, which is why it is inversely proportional to the security term. Moreover, $\nu > (B_{mn} + \eta_{mn} + \Psi_{mn})$ is a parameter to adjust the value of QoS term in the overall utility function. In its generalized form, the Cobb–Douglas function can be written as

$$\tilde{Q}(x) = A\prod_{i=1}^{P} x_i^{\lambda_i} \tag{8}$$

[2] The evolution of malicious software poses a critical challenge to the design of IDSs, which is why we consider a small portion of attacks not to be known to the IDSs.

where $x_1, \dots, x_P$ are the non-negative quantities of goods consumed or produced and λ_i is an elasticity parameter for good i. It should be noted that $\lambda = \sum_{i=1}^{P} \lambda_i$, $\alpha_i = \frac{\lambda_i}{\lambda}$ and $\alpha = \sum_{i=1}^{P} \alpha_i$. Hence, we rewrite (8) as

$$Q(x) = A \prod_{i=1}^{P} x_i^{\alpha_i} \tag{9}$$

Here we recall a feature of Cobb–Douglas production function properties that allows us (or the operator) the degrees of freedom to define α_i according to the parameters of the problem at hand. In order to incorporate elasticity in α_i we define

$$\alpha'_i = \frac{\alpha_i}{1 - \alpha_i} \tag{10}$$

So, (9) integrates elasticity as

$$Q(x) = A \prod_{i=1}^{P} x_i^{\alpha'_i} \tag{11}$$

Considering (7) and (11), the joint security and QoS utility function, where QoS utility function includes bandwidth, computational resources and monetary cost, for a detection level L_m can be defined as

$$Q(L_m) = A \times$$

$$\Big(\rho(L_m) \times H(L_m)\Big)^{\alpha'_1} \times \left(\frac{\nu}{B(L_m) + \eta(L_m) + \Psi(L_m)}\right)^{\alpha'_2} \tag{12}$$

where the first term represents the security function and the second term represents the QoS function.

3.1. The joint optimization problem

The optimization problem for all SAs can be written as

$$\max_{\mathbf{L}_m} \left\{ \sum_{m=1}^{M} Q(L_m) \right\} \tag{13}$$

where $\mathbf{L}_m \in \mathbb{R}^M$ represents the detection level decision vector for the SAs. After removing the total factor productivity parameter,[3] let us rewrite the above problem for finding the decision matrix $\mathbf{X}$ as

$$\mathbf{P1}: \max_{\mathbf{X}} \left\{ \sum_{m=1}^{M} \sum_{n=1}^{N} \left(\Big(\rho_{mn} \times H_{mn}\Big)^{\alpha'_1} \times \left(\frac{\nu}{B_{mn} + \eta_{mn} + \Psi_{mn}}\right)^{\alpha'_2} \right) x_{mn} \right\} \tag{14}$$

subject to

$$\mathbf{C1.1}: \sum_{n=1}^{N} x_{mn} = 1, \quad \forall m, \tag{15}$$

$$\mathbf{C1.2}: \sum_{n=1}^{N} \rho_m x_{mn} \geq \delta_s, \quad \forall m, \tag{16}$$

$$\mathbf{C1.3}: \sum_{m=1}^{M} \sum_{n=1}^{N} B_{mn} x_{mn} \leq \delta_b, \tag{17}$$

$$\mathbf{C1.4}: \sum_{m=1}^{M} \sum_{n=1}^{N} \eta_{mn} x_{mn} \leq \delta_\eta, \tag{18}$$

$$\mathbf{C1.5}: \sum_{m=1}^{M} \sum_{n=1}^{N} \Psi_{mn} x_{mn} \leq \delta_\Psi, \tag{19}$$

$$\mathbf{C1.6}: x_{mn} \in \{0, 1\}, \quad \forall m, n \tag{20}$$

where $\mathbf{X} \in \mathbb{R}^{M \times N}$ is the decision matrix where each element is binary (i.e., $x_{mn} \in \{0, 1\}$) representing if the nth detection level is selected for the mth SA. Constraint (15) assures each SA is assigned only one detection level. Constraint (16) denotes that the security level for each SA should be selected such that it guarantees detection of δ_s% of the cyberattacks. Constraints (17)–(19) ensure that the aggregated bandwidth, computational consumption, and monetary costs, respectively, of the selected levels among the SAs, do not exceed the maximum available network resources.

The optimization problem assigns the detection level to the SAs such that the trade-off between maximizing the security detection efficiency and the QoS is addressed while also ensuring that the constraints are respected. **P1** is a Binary Linear Programming problem. Although in large dimensions it is NP-hard, due to the large coverage of SAs, and even for several hundred SAs it can be solved by using standard solvers such as CPLEX with low execution time on modest hardware [41,42].

3.2. Optimizing elasticity parameters for balancing security and QoS objectives

In mathematical optimization problems, finding the sweet spot or optimal solution is crucial for identifying the best possible solution among a range of alternatives. In our context, we are interested in optimizing elasticity parameters for balancing the security and QoS terms in the joint objective function. This (a) helps in optimizing the system efficiency in allocating different QoS resources (bandwidth, computational and monetary costs) to different SAs by the selection of a proper detection level, (b) ensures that the system operates in a cost-effective manner while meeting the required security objectives, and (c) provides an understanding of the point from which higher security/QoS utility can be obtained by slightly increasing/decreasing the optimal elasticity parameter.

However, in our problem, the security and QoS values are selected based on observations from monitoring tools, and they are not generated randomly or according to a uniform distribution. Therefore, we cannot simply assume that the point $\alpha_1 = \alpha_2 = 0.5$ is the balancing point, as this point varies across different levels and SAs depending on the security and QoS values. To address this issue, we derive the optimal set of elasticity parameters that balance the security and QoS objectives.

The $\alpha_1^{*\prime}$ and $\alpha_2^{*\prime}$ aim to identify the optimal values of α'_1 and α'_2 in the joint objective function where both objectives are equally satisfied. This can be seen as a game-theoretical approach where the two sides of the game try to maximize their own utility function, however, the equilibrium is where both sides are equally satisfied. To determine such values for α'_1 and α'_2, we need to minimize the joint objective function as this is the point where no objective has a higher utility than the other, i.e., the balancing point.

Fig. 2 is a graphical analysis of the joint objective value of three detection levels of an SA using (12). As seen, when $\alpha_2 = 0.9$, Level 1 and 3 have the highest and the lowest utility, respectively, and when $\alpha_1 = 0.9$, Level 3 and 1 have the highest and the lowest utility, respectively. That is, when the QoS is prioritized (i.e., $\alpha_2 = 0.9$), Level 1 is preferred more than the rest and when security is prioritized (i.e., $\alpha_1 = 0.9$), Level 3 is preferred more than the rest. The minimum points of each of these three curves are encircled in the figure, and the respective elasticity parameters represent the optimal values that allow for balancing the security and QoS objectives. If a higher QoS is desired, we can move left to a certain percentage (i.e., $\alpha_1^{*\prime} - \delta$), and if a higher level of security is desired, we can move right (i.e., $\alpha_1^{*\prime} + \delta$). In order to find the optimal elasticity parameters to reach the balancing point for one SA, we calculate the balancing point for each of the detection levels by taking the First-Order Optimality Conditions of **P1** with respect to each of the elasticity parameters and finally select the detection level with the highest joint utility function. Hence, we rewrite (14) as

$$\boldsymbol{\alpha}_1^{*\prime}, \boldsymbol{\alpha}_2^{*\prime} =$$

[3] It does not change the IDM selection output while only changing the value of the joint utility function.

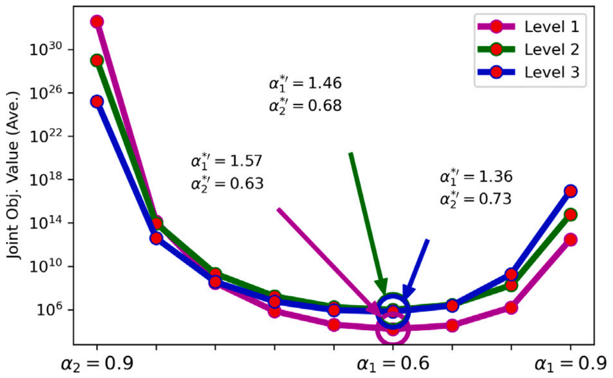


Fig. 2. Optimal elasticity parameters for balancing the objectives.

$$\underset{\alpha'_1,\alpha'_2}{\operatorname{argmin}}\left\{\sum_{m=1}^{M}\sum_{n=1}^{N}\left((Y_m^{\text{Sec}})^{\alpha'_{1,mn}} \times (v/Y_m^{\text{QoS}})^{\alpha'_{2,mn}}\right)\right\} \tag{21}$$

where $\boldsymbol{\alpha}_1^{*\prime}$ and $\boldsymbol{\alpha}_2^{*\prime} \in \mathbb{R}^{M\times N}$. $\boldsymbol{\alpha}_1^{*\prime}$ can be defined as

$$\boldsymbol{\alpha}_1^{*\prime} = \begin{pmatrix} \alpha^{*\prime}_{1,(1,1)} & \alpha^{*\prime}_{1,(1,2)} & \alpha^{*\prime}_{1,(1,3)} \\ \vdots & \vdots & \vdots \\ \alpha^{*\prime}_{1,(3,1)} & \alpha^{*\prime}_{1,(3,2)} & \alpha^{*\prime}_{1,(3,3)} \\ \vdots & \vdots & \vdots \\ \alpha^{*\prime}_{1,(5,1)} & \alpha^{*\prime}_{1,(5,2)} & \alpha^{*\prime}_{1,(5,3)} \end{pmatrix}, \quad \text{where } \alpha^{*}_{1,(m,n)} \in (0,1) \tag{22}$$

$\alpha^{*\prime}_{1,(m,n)}$ represents the security elasticity parameter for the nth level of the mth SA, where the lower index 1 refers to the security elasticity (similarly, 2 in $\boldsymbol{\alpha}_2^{*\prime}$ refers to the QoS elasticity parameter). In Eq. (22), the indices of the level and agent are written in parentheses to avoid confusion with the first index, which represents the objective index. Please note that the elements in the matrix are the elasticity parameters converted from their respective $\alpha^{*}_{1,(m,n)}$ and as stated before $\alpha^{*}_{1,(m,n)} + \alpha^{*}_{2,(m,n)} = 1$. Similar to (22), we can also define $\boldsymbol{\alpha}_2^{*\prime}$.

Proposition 1. *The optimal value of* $\alpha_{1,(m,n)}$*, which balances the objectives in* **P1***, is*

$$\alpha^{*}_{1,(m,n)} = \frac{\sqrt{\ln\left(\frac{v}{B_{mn}+\eta_{mn}+\Psi_{mn}}\right)/\ln(\rho_{mn}\times H_{mn})}}{1+\sqrt{\ln\left(\frac{v}{B_{mn}+\eta_{mn}+\Psi_{mn}}\right)/\ln(\rho_{mn}\times H_{mn})}} \tag{23}$$

Proof. The proof is given in Appendix □

$\alpha^{*}_{2,(m,n)}$ can be calculated as $\alpha^{*}_{2} = 1 - \alpha^{*}_{1}$. Considering Eq. (23) and by using (10), we can obtain the optimal $\alpha_i^{*\prime}$ as

$$\alpha^{*\prime}_{1,(m,n)} = \sqrt{\frac{\ln\left(\frac{v}{B_{mn}+\eta_{mn}+\Psi_{mn}}\right)}{\ln\left(\rho_{mn}\times H_{mn}\right)}} \tag{24}$$

$$\alpha^{*\prime}_{2,(m,n)} = \sqrt{\frac{\ln\left(\rho_{mn}\times H_{mn}\right)}{\ln\left(\frac{v}{B_{mn}+\eta_{mn}+\Psi_{mn}}\right)}} \tag{25}$$

Using (24) and (25), we can obtain $\boldsymbol{\alpha}_1^{*\prime}$ and $\boldsymbol{\alpha}_2^{*\prime}$, and by replacing them into **P1**, we obtain (26) (see Box I), subject to **C1**.**1** – **C1**.**6**. **P2** in its simpler form can also be rewritten as

$$\max_{\mathbf{X}}\left\{\sum_{m=1}^{M}\sum_{n=1}^{N}\left((Y_m^{\text{Sec}})^{\sqrt{\ln\left(\frac{v}{Y_m^{\text{QoS}}}\right)/\ln(Y_m^{\text{Sec}})}} \times (v/Y_m^{\text{QoS}})^{\sqrt{\ln(Y_m^{\text{Sec}})/\ln\left(\frac{v}{Y_m^{\text{QoS}}}\right)}}\right)x_{mn}\right\}$$

Please note that **P1** allows the operator/admin to adjust the importance of the security and QoS objectives, while **P2** automates this process by setting the optimal elasticity parameters such that the balancing point between the two objectives are found.

Our proposed mechanism effectively manages dynamic changes in network conditions and cyber threats for several reasons. These include its consideration of security-related dynamics denoted as $H(L_m)$, QoS-related dynamics represented by $B(L_m), \eta(L_m)$ and $\Psi(L_m)$, as well as the utilization of system-defined security and QoS-related thresholds to regulate detection efficiency and resource management. Furthermore, its adaptability is supported by the properties of the S-type Cobb–Douglas function. The mechanism provides continuous protection under various settings, whether manually configured or automated with regard to security and QoS priorities, all while making real-time decisions.

4. Simulation results

In this section, we present the numerical results obtained through computer simulations, which are performed in *Python*. Notably, simulations have been handled based on a wide range of attacks and threats relevant to 5G networks and 5G-specific protocols (as identified by the EU project SANCUS [43,44]), including NAS-5G SMC Replay attacks, PFCP fraudulent session establishment, deletion or modification requests, SUCI attacks, HTTP2 poisoning attacks, 5G protocol-related denial of service attacks, to name some. To address these threats, several IDMs are implemented specifically designed to detect attacks that primarily target 5G-specific protocols like NGAP, PFCP, and HTTP2. To effectively detect these attacks, our IDMs are equipped with the ability to parse 5G-specific protocols, allowing them to extract relevant fields for analysis. Additionally, our approach incorporates AI/ML-based detection techniques and employs distributed events correlation methods to enhance detection capabilities. These advanced techniques supplement traditional rule-based detection, enabling us to identify more sophisticated attacks, particularly those occurring within encrypted traffic or involving multi-layered attacks.

We have relied on the *Montimage Monitoring Tools* (MMT)[45][4] intrusion detection system that is built to detect intrusions in close-to-real-time by performing soft- and deep-inspection threat analysis and identifying their type and severity. To evaluate the performance of our solution for the IDM selection in a system, we have considered our observations from MMT and have provided a range of values in Table 1 based on expert knowledge of three types of IDMs:

- Level 1 (L1): This level employs a rule-based detection approach, relying on attack signatures' bit-level patterns found in one or more packets. L1 is particularly effective when the attack's signature is well-known, making it a straightforward and efficient mechanism for identifying most common attacks.
- Level 2 (L2): At L2, we harness ML/AI techniques to detect anomalies within the network. These anomalies may be indicative of various attack types, including Distributed Denial of Service (DDoS) attacks. While effective, L2 can be resource-intensive and is primarily geared toward identifying a broader range of attacks.
- Level 3 (L3): L3 is tailored to address complex, multi-faced, and multi-layered attacks. It necessitates the aggregation of data from multiple probes and employs correlation techniques to detect such intricate attacks. L3 is resource-intensive and primarily focuses on a specific set of attacks. However, resource allocation is justified when dealing with high-risk attacks where the potential consequences warrant the investment.

[4] MMT has been used in various metrics (fix/mobile network, home/enterprise/operator, IoT/5G/Cloud, etc.). MMT-5G classifies and weights each detected threat according to the MITRE classification framework and computes the KPI(s) for each threat in the form of a multi-dimensional matrix. The provided values in Table 1 rely on more than 10 years of expertise in network security monitoring.

$$\mathbf{P2}:\max_{\mathbf{X}}\left\{\sum_{m=1}^{M}\sum_{n=1}^{N}\left(\left(\rho_{mn}\times H_{mn}\right)^{\sqrt{\ln\left(\frac{\nu}{H_{mn}c_1+\log\left((1+H_{mn}b)(1+H_{mn}\vartheta)\left(1+H_{mn}c_2\right)\right)}\right)/\ln\left(\rho_{mn}\times H_{mn}\right)}}\right.\right.$$
$$\left.\left.\times\left(\frac{\nu}{H_{mn}c_1+\log\left(\left(1+H_{mn}b\right)\left(1+H_{mn}\vartheta\right)\left(1+H_{mn}c_2\right)\right)}\right)^{\sqrt{\ln(\rho_{mn}\times H_{mn})/\ln\left(\frac{\nu}{H_{mn}c_1+\log\left((1+H_{mn}b)(1+H_{mn}\vartheta)\left(1+H_{mn}c_2\right)\right)}\right)}}\right)\times x_{mn}\right\} \tag{26}$$

Box I.

Table 1
SA security and QoS parameters setting.

Levels	$\zeta(L_m)$	$b(L_m)$ (per attack)	$\vartheta(L_m)$ (per attack)	c_1 (per attack)	c_2 (per attack)
L1 (signature-based)	[86 90]%	0.001	(0 0.1]	[0.05 0.3]	[0.003 0.007]
L2 (anomaly-based)	[91 93]%	0.001	[0.8 0.9]	[0.15 0.7]	[0.008 0.02]
L3 (hybrid)	[94 95]%	(0 0.1]	[0.9 1]	[0.7 0.99]	[0.008 0.02]

Our algorithm's deployment can be achieved by the following scheme structure compatible with the 5G setting:

1. the algorithm is encoded as a Python program and it is containerized as a Virtual Machine (VM) using Docker/Kubernetes,
2. the VM is conducted within the Management and Orchestration (MANO) framework of the 5G Core,
3. the VM receives (A) security-related data by providing inputs to connect to other VMs situated at the MANO system for security-scanning, threat analysis, etc., (like MMT-5G), and (B) service-related data through a user interface,
4. the VM realizes the changes at the input data via time- or event-triggering modules (dockerized in the MANO),
5. upon triggering, the VM performs the Security-vs-QoS optimization (i.e number and levels of SAs to be allocated in the underlying 5G system),
6. the VM provides the output to the Security Orchestrator as a multi-dimensional matrix with elements for each threat detected and each user requirement changed,
7. the Security Orchestrator decodes the matrix and communicates with the MANO Orchestrator,
8. the MANO deploys the optimal result in the underlying 5G system network via REST API.

Yet, we stress that the deployment of such schemes and the coordination mechanism between the SAs are out of the scope of this work, which focuses on the design and math-based solution of the proposed trade-off problem. In order to study the IDM selection problem, we have considered a pre-deployment of SAs in a given area. The primary objective is to comprehensively cover the relevant network paths. This allows each SA to monitor the network elements within their respective coverage zone.

Each SA has 3 detection levels corresponding to signature-based, anomaly-based, and hybrid IDMs. Moreover, 5% of the cyberattacks are considered unknown (i.e., $\imath = 5$). All Sec and QoS terms are normalized to fall within the (0 1) range, as provided in the table. On one hand, constraint (16) enforces the selection of higher detection levels, on the other hand, the (17)–(19) QoS constraints set budget limitations on the selection of higher levels, creating a trade-off that must be addressed. In the following, we perform several experiments to demonstrate the impact of different parameters on the IDM selection process.

4.1. Impact of δ_s on the selected IDM

This experiment examines the impact of various δ_s values on the selection of detection levels and the number of feasible solutions (i.e., the number of detection levels satisfying the security constraint), with a generous amount of QoS resources. To accomplish this, we relax the total number of attacks to $H' = 30$, assume the number of agents is $M = 5$, $\alpha_1 = 0.7$, $\alpha_1 = 0.3$, and randomly select QoS values within the ranges provided in Table 1. The maximum QoS values are used to calculate the QoS budget ensuring it never restricts the detection level selection process. The average of 100 simulation runs for 5 SAs is depicted in Fig. 3.

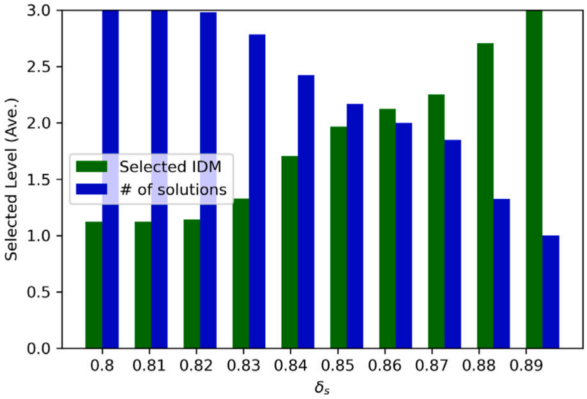


Fig. 3. Impact of δ_s on IDM selection of SAs and the number of feasible solutions.

The figure indicates that when δ_s is small, all three levels are feasible. However, since the objective considers both security and QoS, lower-level IDMs are preferred (for higher security selection, the α_1 needs to be set higher). Conversely, when the δ_s constraint is set to 0.89, only one level is feasible (only the highest level guarantees a security detection level higher than 0.89), which is always selected. Thus, the δ_s value can determine the number of feasible solutions, with a tighter value limiting the feasibility to only the highest levels, and a more generous value resulting in all IDM being feasible, with selection dependent on the importance of security and QoS.

4.2. Impact of $\delta_b, \delta_\eta, \delta_\psi$ on the selected IDM

In this experiment, we relax the security constraint while considering various QoS values to see the impact of QoS metrics on the selection of detection levels. To this end, we relax the number of attacks to $H' = 30$, the number of agents to $M = 5$, and the security and QoS values are randomly selected from the ranges given in Table 1. A low

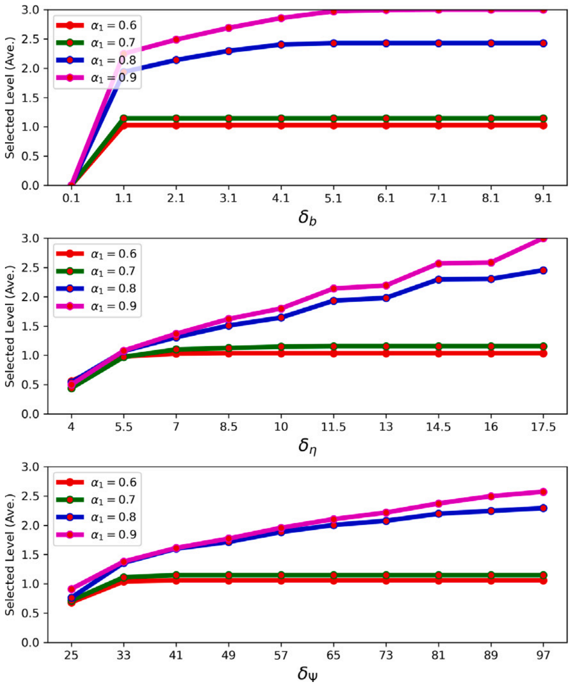


Fig. 4. Impact of δ_b, δ_η and δ_Ψ on IDM selection of SAs.

security requirement is used ensuring it never restricts the detection selection process. The average of 100 simulation runs[5] for 5 SAs with different α_1 values is depicted in Fig. 4.

The results show that when δ_* is small the lowest levels are selected. This is because, with a low QoS budget, only the lowest detection level is feasible. However, as the QoS budget increases (i.e., higher δ_*), higher detection levels become feasible as they consume more QoS resources, and the curves rise. It is important to note the selection of a detection level with high QoS budgets also depends on the α_1 and α_2. For instance, even if a large QoS budget is available but $\alpha_1 = 0.6$, lower detection levels are selected as QoS is prioritized over the security in the joint objective function. On the other hand, for $\alpha_1 = 0.9$, higher detection levels are preferred as security is prioritized more. Please note as the bandwidth values in all three levels, as given in Table 1, are small, a bandwidth budget of $\delta_b = 0.1$ does not result in a feasible solution and for the values of $\delta_b > 0.1$ nearly all levels become feasible.

4.3. Impact of α_i on the selected IDM

In this experiment, we relax the security and QoS constraints while various α_i values to see the impact of elasticity parameters on the selection of detection levels. Please note that the values of elasticity parameters are calculated by inserting α_1 and α_2 into (10). We also relax the number of attacks to be $H' = 30$, the number of agents to be $M = 5$, and the security and QoS values are randomly selected from the ranges given in Table 1. Low security and high QoS requirements are used ensuring they are not restricting the detection selection process. The average of 100 simulation runs for 5 SAs is depicted in Fig. 5.

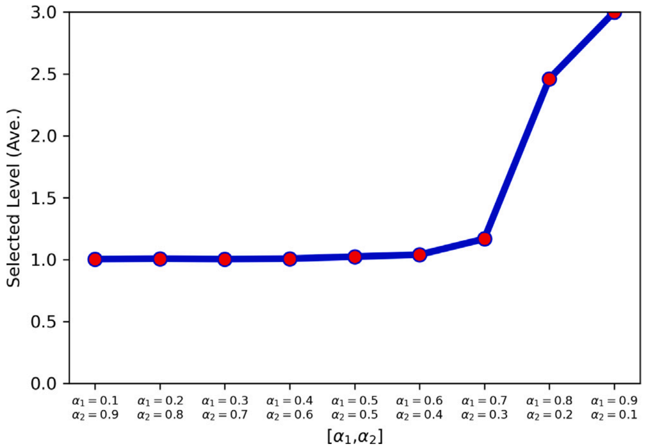


Fig. 5. Impact of α_i on IDM selection of SAs.

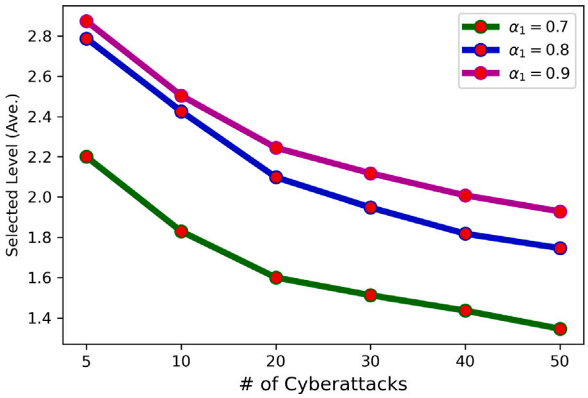


Fig. 6. Impact of number of cyberattacks on the selection of IDMs.

It is worth noting that both security and QoS are considered in the objective function of the above curves, however, different importance is given in the joint objective function. It can be seen as the α_1 increases, indicating a higher priority for security, higher detection levels are selected. It is important to highlight that, based on the current IDMs and their corresponding security and QoS values, setting $\alpha_1 > 0.7$ is necessary to prioritize security over QoS.

4.4. Impact of number of cyberattacks on the selected IDM

This experiment aims to investigate the impact of the number of cyberattacks on the selection of IDMs while automating security and QoS constraint boundary values. We begin with stringent security and QoS constraints and test the feasibility of finding a solution. If a feasible solution is found, we return it; otherwise, we slightly loosen the constraints. This iterative process of relaxing the constraints continues until a feasible solution is obtained. The average of 100 simulation runs for 5 SAs is depicted in Fig. 6.

The impact of the number of cyberattacks is observed on the increase of the QoS costs and therefore, on the feasible solution sets. As seen, by the increase in the number of cyberattacks, the lower IDMs are selected more often. This is because as more attacks are detected, the associated QoS costs also increase. As a result, only the lower-level IDMs that meet the QoS requirements remain as feasible solutions. Additionally, we can also see that when $\alpha_1 = 0.9$, it tends to favor the selection of higher-level IDMs.

4.5. Impact of number of SAs on the time complexity of the solution

This experiment aims to investigate the impact of the number of SAs on the time complexity of the solution while automating security and QoS constraint values as explained in Section 4.4. The average of 50 simulation runs is depicted in Fig. 7. Please note, different values of α_1

[5] Please note the values are an average of 100 runs for 5 SAs; hence, the selected level values of smaller than level 1, indicate that in some of the runs, no feasible solution was found.

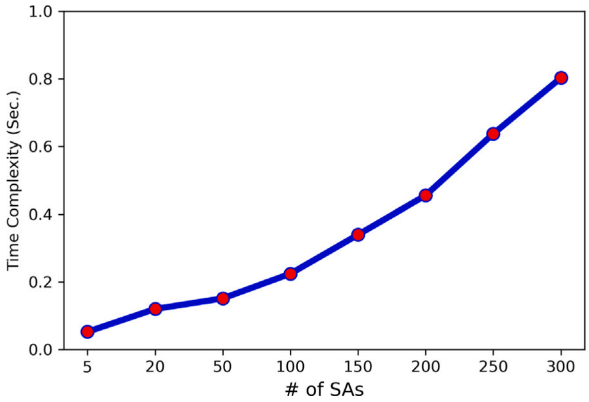


Fig. 7. Impact of number of SAs on the time complexity of the solution.

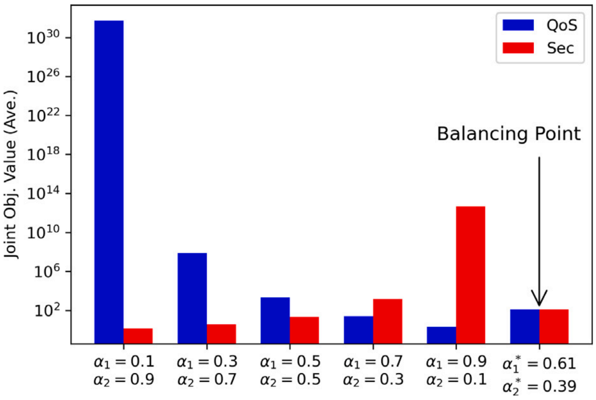


Fig. 8. The security and QoS objective values and the balancing point obtained through the optimal elasticity parameters.

and H' do not have any impact on the time complexity of the solution but on the IDM selection.

As seen, as the number of SAs increases the average time complexity of obtaining the optimal solution with feasible security and QoS bounds rises, which is expected. It is important to highlight that each SA covers the monitoring of a certain area, and therefore, 300 SAs may represent the coverage of several states in a country, which is a large area. The time complexity presented in the above results is obtained by running the code on modest hardware. However, when executed on a server with higher computational complexity, the optimal solution for all SAs can be obtained in much less than 0.5 s. This demonstrates that the optimal solution can be found quickly, considering both time and energy consumption, even for a large number of SAs.

4.6. *Optimal elasticity parameters for obtaining the balancing point*

In this experiment, we relax the Security and QoS constraints to observe the impact of different $[\alpha_1, \alpha_2]$ values on the security and QoS utility terms individually. The average of 100 simulation runs is depicted in Fig. 8. The elasticity values in this figure are converted to their corresponding $[\alpha_1, \alpha_2]$ values in the X-axis.

The figure[6] confirms that a high α_2 value leads to a very high QoS utility but a low security utility, which explains the selection of level 1 in Fig. 5. In contrast, a high security power value, i.e., $\alpha_1 = 0.9$, results in the highest achievable security utility and explains the selection of Level 3 in Fig. 5. However, the most balanced outcome can be achieved by solving (26) in Box I using (22), where both objectives have the same utility value. This demonstrates that $\boldsymbol{\alpha}'_1$ and $\boldsymbol{\alpha}'_2$ can find the balancing point.

The study leads to the following conclusions: (a) when α'_1 is very close to zero, the optimal objective is achieved, but security will have a low impact in such cases; (b) the most balanced objective can be achieved by utilizing the derived $[\boldsymbol{\alpha}'_1, \boldsymbol{\alpha}'_2]$; and (c) to encourage the selection of level 3, an $\alpha_1 \geq 0.8$ is needed. It should be noted that these conclusions are specific to the case study analyzed in this paper.

5. Conclusion

In this study, we addressed the problem of SA detection level selection where the SAs perform the system monitoring for intrusion detection. We considered a scenario where multiple SAs can monitor the system at different detection levels, with higher levels offering better accuracy but at a higher cost. We formulated the joint security and QoS optimization problem using the Cobb–Douglas production function, which is a unique approach in this field. We conducted simulations and analyzed the impact of various parameters on the IDM selection. Our findings show that certain elasticity parameter values allow for the selection of higher and lower detection levels. Additionally, we analytically determined the optimal elasticity parameter values to strike a balance between the two objectives. We also illustrated how the number of attacks, as well as various security and QoS budget values, affect the selection of the IDMs.

In the future, we aim to study the problem of SA deployment in a 5G environment and examine the ramifications of multiple SAs operating in overlapping regions. Moreover, we target exploring a more complex scenario by investigating the impact of increasing the number of IDMs for network monitoring, while also integrating additional QoS factors into the utility function.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Arash Bozorgchenani, Qiang Ni, Charilaos C. Zarakovits and Wissam Mallouli reports financial support was provided by Horizon Europe.

Data availability

The data used for obtaining the results is shown on Table 1 in the Simulation Results section.

Acknowledgment

This research is supported by the H2020 SANCUS project under grant number GA952672.

Appendix. Optimal α_1

For the sake of simplicity in the notation, the indices of n and m are removed from the α_i in this section. From (10), we have $\alpha'_1 = \frac{\alpha_1}{1-\alpha_1}$ and $\alpha'_2 = \frac{\alpha_2}{1-\alpha_2} = \frac{1-\alpha_1}{\alpha_1}$. Let us, for the sake of simplicity in notation, write $S = \rho_{mn} \times H_{mn}$ and $Q = \frac{\nu}{B_{mn}+\eta_{mn}+\Psi_{mn}}$. We can rewrite the security and QoS terms as a function of α_i as

$$s(\alpha_1) = S^{\frac{\alpha_1}{1-\alpha_1}} \tag{A.1}$$

and

$$q(\alpha_1) = Q^{\frac{1-\alpha_1}{\alpha_1}} \tag{A.2}$$

[6] Please note that a high value of ν is selected for plotting this figure, which is why the QoS utility for the case $\alpha_2 = 0.9$ has a higher value than the security utility for the case of $\alpha_1 = 0.9$. Decreasing the value of ν results in a higher value of security utility. However, regardless of the value of ν, the selection of IDM is the same, i.e., it changes the joint objective value, but not the selected IDM as it is present in all the detection levels.

The derivation for the above functions with respect to α_1 are

$$s'(\alpha_1) = S^{\frac{\alpha_1}{1-\alpha_1}} \cdot \frac{\ln S}{(1-\alpha_1)^2} \tag{A.3}$$

and

$$q'(\alpha_1) = -\frac{Q^{\frac{1-\alpha_1}{\alpha_1}}}{\alpha_1^2} \cdot \ln Q \tag{A.4}$$

Substituting (A.1) and (A.2) in **P1** yields

$$f(\alpha_1) = S^{\frac{\alpha_1}{1-\alpha_1}} \times Q^{\frac{1-\alpha_1}{\alpha_1}} \tag{A.5}$$

Applying the chain rule for the derivation of $f(\alpha_1)$ considering (A.3) and (A.4) yields

$$\frac{\partial f(\alpha_1)}{\partial \alpha_1} = \left(S^{\frac{\alpha_1}{1-\alpha_1}} \cdot q'(\alpha_1) \right) + \left(Q^{\frac{1-\alpha_1}{\alpha_1}} \cdot s'(\alpha_1) \right) = \left(-\frac{S^{\frac{\alpha_1}{1-\alpha_1}} Q^{\frac{1-\alpha_1}{\alpha_1}}}{\alpha_1^2} \cdot \ln Q \right) + \left(\frac{S^{\frac{\alpha_1}{1-\alpha_1}} Q^{\frac{1-\alpha_1}{\alpha_1}}}{(1-\alpha_1)^2} \cdot \ln S \right) \tag{A.6}$$

To find the minimum value of $f(\alpha_1)$ we set $\frac{\partial f(\alpha_1)}{\partial \alpha_1} = 0$, which yields

$$\frac{S^{\frac{\alpha_1}{1-\alpha_1}} Q^{\frac{1-\alpha_1}{\alpha_1}}}{(1-\alpha_1)^2} \cdot \ln S = \frac{S^{\frac{\alpha_1}{1-\alpha_1}} Q^{\frac{1-\alpha_1}{\alpha_1}}}{\alpha_1^2} \cdot \ln Q \tag{A.7}$$

$$\frac{\ln S}{(1-\alpha_1)^2} = \frac{\ln Q}{\alpha_1^2} \tag{A.8}$$

After some algebraic calculations the optimal α_1 equals

$$\alpha_1 = \frac{\sqrt{\frac{\ln Q}{\ln S}}}{\left(1 + \sqrt{\frac{\ln Q}{\ln S}}\right)} \tag{A.9}$$

This completes the proof.

References

[1] M.A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, H. Janicke, Security for 4 g and 5 g cellular networks: A survey of existing authentication and privacy-preserving schemes, J. Netw. Comput. Appl. 101 (2018) 55–82, http://dx.doi.org/10.1016/j.jnca.2017.10.017.

[2] R. Khan, P. Kumar, D.N.K. Jayakody, M. Liyanage, A survey on security and privacy of 5 g technologies: Potential solutions, recent advancements, and future directions, IEEE Commun. Surv. Tutor. 22 (1) (2020) 196–248, http://dx.doi.org/10.1109/COMST.2019.2933899.

[3] Z. Yang, X. Liu, T. Li, D. Wu, J. Wang, Y. Zhao, H. Han, A systematic literature review of methods and datasets for anomaly-based network intrusion detection, Comput. Secur. 116 (2022) 102675, http://dx.doi.org/10.1016/j.cose.2022.102675.

[4] K.A. Garcia, R. Monroy, L.A. Trejo, C. Mex-Perera, E. Aguirre, Analyzing log files for postmortem intrusion detection, IEEE Trans. Syst. Man Cybern. C 42 (6) (2012) 1690–1704, http://dx.doi.org/10.1109/TSMCC.2012.2217325.

[5] M. Zineddine, Optimizing security and quality of service in a real-time operating system using multi-objective bat algorithm, Future Gener. Comput. Syst. 87 (2018) 102–114, http://dx.doi.org/10.1016/j.future.2018.02.043.

[6] P.H. Mirzaee, M. Shojafar, H. Bagheri, T.H. Chan, H. Cruickshank, R. Tafazolli, A two-layer collaborative vehicle-edge intrusion detection system for vehicular communications, in: 2021 IEEE 94th Vehicular Technology Conference, VTC2021-Fall, 2021, pp. 1–6, http://dx.doi.org/10.1109/VTC2021-Fall52928.2021.9625388.

[7] A. Gupta, R.K. Jha, P. Gandotra, S. Jain, Bandwidth spoofing and intrusion detection system for multistage 5 g wireless communication network, IEEE Trans. Veh. Technol. 67 (1) (2018) 618–632, http://dx.doi.org/10.1109/TVT.2017.2745110.

[8] H. Ji, Y. Wang, H. Qin, Y. Wang, H. Li, Comparative performance evaluation of intrusion detection methods for in-vehicle networks, IEEE Access 6 (2018) 37523–37532, http://dx.doi.org/10.1109/ACCESS.2018.2848106.

[9] R. Parsamehr, A. Esfahani, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, J.-F. Martínez-Ortega, A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells, IEEE Trans. Comput. Soc. Syst. 6 (6) (2019) 1467–1477, http://dx.doi.org/10.1109/TCSS.2019.2949153.

[10] M. Lin, B. Zhao, Q. Xin, Erid: A deep learning-based approach towards efficient real-time intrusion detection for iot, in: 2020 IEEE Eighth International Conference on Communications and Networking, ComNet, 2020, pp. 1–7, http://dx.doi.org/10.1109/ComNet47917.2020.9306110.

[11] T. Taleb, Y. Hadjadj-Aoul, Qos2: a framework for integrating quality of security with quality of service, Secur. Commun. Netw. 5 (12) (2012) 1462–1470, http://dx.doi.org/10.1002/sec.523, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.523 URL https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.523.

[12] X. Zhao, Q. Lin, J. Chen, X. Wang, J. Yu, Z. Ming, Optimizing security and quality of service in a real-time database system using multi-objective genetic algorithm, Expert Syst. Appl. 64 (2016) 11–23, http://dx.doi.org/10.1016/j.eswa.2016.07.023, URL https://www.sciencedirect.com/science/article/pii/S0957417416303694.

[13] Z.M. Fadlullah, C. Wei, Z. Shi, N. Kato, Gt-qosec: A game-theoretic joint optimization of qos and security for differentiated services in next generation heterogeneous networks, IEEE Trans. Wireless Commun. 16 (2) (2017) 1037–1050, http://dx.doi.org/10.1109/TWC.2016.2636186.

[14] Z. Sun, Y. Liu, J. Wang, R. Yu, D. Cao, Cross-layer tradeoff of qos and security in vehicular ad hoc networks: A game theoretical approach, Comput. Netw. 192 (2021) 108031, http://dx.doi.org/10.1016/j.comnet.2021.108031, URL https://www.sciencedirect.com/science/article/pii/S1389128621001390.

[15] A. Bozorgchenani, C.C. Zarakovitis, S.F. Chien, Q. Ni, A. Gouglidis, W. Mallouli, H.S. Lim, Joint security-vs-qos game theoretical optimization for intrusion response mechanisms for future network systems, 2023, arXiv:2303.08544.

[16] A. Bozorgchenani, C.C. Zarakovitis, S.F. Chien, H.S. Lim, Q. Ni, A. Gouglidis, W. Mallouli, Joint security-vs-qos framework: Optimizing the selection of intrusion detection mechanisms in 5 g networks, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22, Association for Computing Machinery, New York, NY, USA, 2022, http://dx.doi.org/10.1145/3538969.3544480.

[17] P.V. Ansam Khraisat, Iqbal. Gondal, J. Kamruzzaman, Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecurity 2 (2019) http://dx.doi.org/10.1186/s42400-019-0038-7.

[18] L.N. Tidjon, M. Frappier, A. Mammar, Intrusion detection systems: A cross-domain overview, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3639–3681, http://dx.doi.org/10.1109/COMST.2019.2922584.

[19] M. Nuaimi, L.C. Fourati, B.B. Hamed, Intelligent approaches toward intrusion detection systems for industrial internet of things: A systematic comprehensive review, J. Netw. Comput. Appl. 215 (2023) 103637, http://dx.doi.org/10.1016/j.jnca.2023.103637.

[20] B.B. Gupta, S. Srinivasagopalan, Handbook of Research on Intrusion Detection Systems, 2020, p. 407, http://dx.doi.org/10.4018/978-1-7998-2242-4.

[21] M.A. Siddiqi, W. Pak, Tier-based optimization for synthesized network intrusion detection system, IEEE Access 10 (2022) 108530–108544, http://dx.doi.org/10.1109/ACCESS.2022.3213937.

[22] M.B. Gorzałczany, F. Rudziński, Intrusion detection in internet of things with mqtt protocol—an accurate and interpretable genetic-fuzzy rule-based solution, IEEE Internet Things J. 9 (24) (2022) 24843–24855, http://dx.doi.org/10.1109/JIOT.2022.3194837.

[23] M.A. Siddiqi, W. Pak, An agile approach to identify single and hybrid normalization for enhancing machine learning-based network intrusion detection, IEEE Access 9 (2021) 137494–137513, http://dx.doi.org/10.1109/ACCESS.2021.3118361.

[24] S.-W. Lee, H. Mohammed sidqi, M. Mohammadi, S. Rashidi, A.M. Rahmani, M. Masdari, M. Hosseinzadeh, Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review, J. Netw. Comput. Appl. 187 (2021) 103111, http://dx.doi.org/10.1016/j.jnca.2021.103111.

[25] N. Shone, T.N. Ngoc, V.D. Phai, Q. Shi, A deep learning approach to network intrusion detection, IEEE Trans. Emerg. Top. Comput. Intell. 2 (1) (2018) 41–50, http://dx.doi.org/10.1109/TETCI.2017.2772792.

[26] M.M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, G. Fortino, A hybrid deep learning model for efficient intrusion detection in big data environment, Inform. Sci. 513 (2020) 386–396, http://dx.doi.org/10.1016/j.ins.2019.10.069.

[27] M.A. Khan, Hcrnnids: Hybrid convolutional recurrent neural network-based network intrusion detection system, Processes 9 (5) (2021) http://dx.doi.org/10.3390/pr9050834.

[28] B. Cao, C. Li, Y. Song, Y. Qin, C. Chen, Network intrusion detection model based on cnn and gru, Appl. Sci. 12 (9) (2022) http://dx.doi.org/10.3390/app12094184, URL https://www.mdpi.com/2076-3417/12/9/4184.

[29] S.M. Kasongo, A deep learning technique for intrusion detection system using a recurrent neural networks based framework, Comput. Commun. 199 (2023) 113–125, http://dx.doi.org/10.1016/j.comcom.2022.12.010.

[30] K. Yadav, B. Gupta, C.-H. Hsu, K.T. Chui, Unsupervised federated learning based iot intrusion detection, in: 2021 IEEE 10th Global Conference on Consumer Electronics, GCCE, 2021, pp. 298–301, http://dx.doi.org/10.1109/GCCE53005.2021.9621784.

[31] L. Zhang, S. Jiang, X. Shen, B.B. Gupta, Z. Tian, PWG-IDS: an intrusion detection model for solving class imbalance in iiot networks using generative adversarial networks, 2021, CoRR abs/2110.03445.

[32] A. Mourad, H. Tout, O.A. Wahab, H. Otrok, T. Dbouk, Ad hoc vehicular fog enabling cooperative low-latency intrusion detection, IEEE Internet Things J. 8 (2) (2021) 829–843, http://dx.doi.org/10.1109/JIOT.2020.3008488.

[33] A. Cardenas, J. Baras, K. Seamon, A framework for the evaluation of intrusion detection systems, in: 2006 IEEE Symposium on Security and Privacy, S & P'06, 2006, pp. 15pp.–77, http://dx.doi.org/10.1109/SP.2006.2.

[34] M. Prasad, S. Tripathi, K. Dahal, An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks, Eng. Appl. Artif. Intell. 119 (2023) 105760, http://dx.doi.org/10.1016/j.engappai.2022.105760, URL https://www.sciencedirect.com/science/article/pii/S0952197622007503.

[35] D. Stiawan, A. Heryanto, A. Bardadi, D.P. Rini, I.M.I. Subroto, Kurniabudi, M.Y.B. Idris, A.H. Abdullah, B. Kerim, R. Budiarto, An approach for optimizing ensemble intrusion detection systems, IEEE Access 9 (2021) 6930–6947, http://dx.doi.org/10.1109/ACCESS.2020.3046246.

[36] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, H. Karimipour, Cyber intrusion detection by combined feature selection algorithm, J. Inf. Secur. Appl. 44 (2019) 80–88, http://dx.doi.org/10.1016/j.jisa.2018.11.007, URL https://www.sciencedirect.com/science/article/pii/S2214212618304617.

[37] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani, M. Hamdi, Tidcs: A dynamic intrusion detection and classification system based feature selection, IEEE Access 8 (2020) 95864–95877, http://dx.doi.org/10.1109/ACCESS.2020.2994931.

[38] Z. Ling, Z.J. Hao, An intrusion detection system based on normalized mutual information antibodies feature selection and adaptive quantum artificial immune system, Int. J. Semant. Web Inf. Syst. 18 (1) (2022) 1–25, http://dx.doi.org/10.4018/IJSWIS.308469.

[39] Z. Ling, Z.J. Hao, Intrusion detection using normalized mutual information feature selection and parallel quantum genetic algorithm, Int. J. Semant. Web Inf. Syst. 18 (1) (2022) 1–24, http://dx.doi.org/10.4018/IJSWIS.307324.

[40] J. Black, N. Hashimzade, G. Myles, Dictionary of Economics, Oxford University Press, 2009.

[41] A. Bozorgchenani, S. Maghsudi, D. Tarchi, E. Hossain, Computation offloading in heterogeneous vehicular edge networks: On-line and off-policy bandit solutions, IEEE Trans. Mob. Comput. (2021) 1, http://dx.doi.org/10.1109/TMC.2021.3082927.

[42] A. Bozorgchenani, D. Tarchi, W. Cerroni, On-demand service deployment strategies for fog-as-a-service scenarios, IEEE Commun. Lett. 25 (5) (2021) 1500–1504, http://dx.doi.org/10.1109/LCOMM.2021.3055535.

[43] S. Project, Sancus: analysis software scheme of uniform statistical sampling, audit and defence processes, 2020-2023, URL https://cordis.europa.eu/project/id/952672.

[44] C. Zarakovitis, D. Klonidis, Z. Salazar, A. Prudnikova, A. Bozorgchenani, Q. Ni, C. Klitis, G. Guirgis, A. Cavalli, N. Sgouros, E. Makri, A. Lalas, K. Votis, G. Amponis, W. Mallouli, Sancus: Multi-layers vulnerability management framework for cloud-native 5 g networks, in: The 16th International Conference on Availability, Reliability and Security, ARES 2021, Association for Computing Machinery, New York, NY, USA, 2021, http://dx.doi.org/10.1145/3465481.3470092.

[45] Montimage Monitoring Tool, URL https://www.montimage.com/products/MMT_Brochure.pdf.

Arash Bozorgchenani is an Assistant Professor (lecturer) in the School of Computing at University of Leeds, UK. He received B.Sc. and M.Sc. degrees in IT in 2013 and 2016, respectively, in Iran, and the Ph.D. degree in Telecommunications and IT from the University of Bologna, Italy, in 2020. He was a visiting researcher at the University of Manitoba, Canada in 2019. He held a postdoctoral position at the University of Bologna in 2020 and during 2020-2023, he served as a Research Associate at Lancaster University, UK. Dr. Bozorgchenani has been involved in both national Gaucho (PRIN 2015, Italy) and European (H2020 SANCUS) projects. He has been TPC member, session chair and organizing member of IEEE flagship conferences. His research interests revolve around Resource Allocation, Optimization and Machine Learning techniques in Wireless Communications and Future Networked Systems (B5G/6G).

Charilaos Zarakovitis is with the Institute of Informatics and Telecommunications, NCSR "Demokritos", and Head of the R&D Department of axon logic, Greece. His research interests include quantum neural networks, machine and deep learning, green communications modeling, bioinspired and game-theoretic decision-making, cognitive radios, network virtualization, statistical signal processing, and convex optimization analysis.

Su Fong Chien was born in Melaka, Malaysia, in 1970. He received the B.Sc. and M.Sc. degrees from University of Malaya, Malaysia, in 1995 and 1998, respectively, and the Ph.D. degree from Multimedia University, Malaysia, in 2002. He is a principal researcher at the Advanced Intelligence Lab in Mimos Berhad, Malaysia. He has published several of tens of conference and refereed journal papers and holds a few patents. He is one of the chief-in editors of Bio-Inspired Computation in Telecommunications. His research interests include optimization in wireless communications via conventional mathematical methods or machine learning and quantum machine learning applications.

Tiew On Ting is with the Department of Media and Technology, Stony Brook Institute at Anhui University (SBIAHU), Anhui University, Hefei City, Anhui Province, P.R. China. He obtained First-Class Honors Degree in Electronic & Telecommunication Engineering from University of Sarawak (UNIMAS), Sarawak, Malaysia; Master of Science from Multimedia University (MMU), Malacca, Malaysia; and Ph.D. Degree in Electrical Engineering from the Hong Kong Polytechnic University, Kowloon, Hong Kong S.A.R. Currently, Ting published a total of 88 scientific papers in the field of optimization, with applications in three major areas: Telecommunication, Power System, and Computer Science. He is well-versed in a wide range of optimization techniques (both conventional and contemporary methods) in solving real-world optimization problems.

Qiang Ni is a Professor at the School of Computing and Communications, Lancaster University, U.K. His research areas include future generation communications and networking, including green communications/networking, millimeter-wave wireless, cognitive radio systems, 5G/6G, SDN, cloud networks, edge computing, dispersed computing, IoT, cyber physical systems, AI/machine learning and vehicular networks. He has authored or co-authored 300+ papers in these areas. He was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to various IEEE wireless standards.

DR. Wissam Mallouli is currently the CTO of Montimage company located in Paris, France. He got his Telecommunication Engineer degree from the National Institute of Telecommunication (INT) in 2005 and his Ph.D. in cybersecurity from Telecom and Management SudParis (France) in 2008. His expertise covers continuous risk management and cyberdefence for critical systems and networks including cloud-based systems, IoT and 4G/5G networks. He is also a professional trainer, and he is working in several collaborative European research projects and has more than 50 scientific publications in popular conferences and journals.