

## SURVEY

# A Systematic Mapping Study on Intrusion Response Systems

ADEL REZAPOUR<sup>1</sup>, MOHAMMAD GHASEMIGOL<sup>2</sup>, AND DANIEL TAKABI<sup>2</sup>, (Member, IEEE)

<sup>1</sup>Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Birjand Branch, Birjand 9717811111, Iran

<sup>2</sup>School of Cybersecurity, Old Dominion University, Norfolk, VA 23529, USA

Corresponding author: Mohammad GhasemiGol (mghasemi@odu.edu)

This work was supported in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber research & development, innovation, and workforce development. For more information about CCI, visit [cyberinitiative.org](http://cyberinitiative.org).

**ABSTRACT** With the increasing frequency and sophistication of network attacks, network administrators are facing tremendous challenges in making fast and optimum decisions during critical situations. The ability to effectively respond to intrusions requires solving a multi-objective decision-making problem. While several research studies have been conducted to address this issue, the development of a reliable and automated Intrusion Response System (IRS) remains unattainable. This paper provides a Systematic Mapping Study (SMS) for IRS, aiming to investigate the existing studies, their limitations, and future directions in this field. A novel semi-automated research methodology is developed to identify and summarize related works. The innovative approach not only streamlines the process of literature review in the IRS field but also has the potential to be adapted and implemented across a variety of research fields. As a result of this methodology, 287 papers related to the IRS were identified from a pool of 6143 studies extracted by the developed web robot based on initial keywords. This highlights its effectiveness in navigating and extracting valuable insights from the extensive body of literature. Furthermore, this research methodology allows the identification of prominent researchers, journals, conferences, and high-quality papers in the field of study.


**INDEX TERMS** Intrusion detection system, intrusion response system, systematic mapping study.

## I. INTRODUCTION

In today's interconnected world, the increasing sophistication of cyber threats poses significant challenges to the security of computer networks. Attackers are constantly finding new ways to infiltrate and compromise networks, making it essential to develop robust and effective security solutions. An IRS is an integral component of the defense life-cycle that focuses on responding to detected intrusions by selecting appropriate countermeasures [1]. Designing an effective IRS presents several challenges [2]. One of the key challenges is accurately estimating the cost of response and selecting the optimal response that aligns with network performance requirements. The selected response should effectively mitigate intrusions while minimizing disruptions to legitimate network traffic. Making the wrong choice can lead to unintended consequences such as denying access to authorized

users or decreasing overall network performance. Dealing with the high volume of alerts generated by Intrusion Detection Systems (IDS) and minimizing the time between intrusion detection and response selection are other important challenges faced by intrusion detection systems.

In recent years, many research works have been published to address these challenges in IRS design. However, the development of an effective multi-objective response system that can address these challenges remains a prominent issue in this field. Also, a study has not been conducted to evaluate and determine the gaps between these issues. Reviewing this literature requires the use of a research method. Two research methods in the literature review are systematic mapping study (SMS) and systematic literature review (SLR) [3], [4]. SLRs and SMSs have different objectives. SLRs involve in-depth studies of narrow areas, using specific research questions and meta-analysis to generate new knowledge. On the other hand, SMSs aim to provide comprehensive overviews and mappings of broader research fields. Therefore, when the goal is

The associate editor coordinating the review of this manuscript and approving it for publication was Xiali Hei .

**TABLE 1.** Taxonomy of existing IRSs (primary studies).

Title	Year	Reference
A Taxonomy and implementation of automated responses to intrusive behavior	1996	[5]
An Intrusion Response Taxonomy and its Role in Automatic Intrusion Response	2000	[2]
A new automatic intrusion response taxonomy and its application	2006	[6]
A taxonomy of intrusion response systems	2007	[7]
Towards a Temporal Response Taxonomy	2012	[8]
Intrusion response systems: survey and taxonomy	2012	[9]
Taxonomy of intrusion risk assessment and response system	2014	[10]

to determine and categorize studies within a specific field, an SMS is used to map the related studies to identified categories and topics. The process of conducting an SMS involves defining research questions, planning the study, conducting a comprehensive literature search, screening and extracting data from related studies, analyzing the data, assessing study quality, and reporting the findings. The objective of this paper is to provide an SMS that comprehensively investigates IRSs, addressing challenges, advancements, and future directions. Some studies have presented various categories for IRSs based on automation level, collaboration capability, response cost, response time, response selection, and collaboration capability, as listed in Table 1. We utilize these studies to initiate our search process.

The main contributions of this paper are as follows:

- This paper presents a comprehensive SMS addressing the limitations and challenges of IRS and provides a roadmap for researchers interested in conducting research in this field.
- A web robot is developed to automate the search process for related studies across diverse resources including journals, conferences, workshops, books, technical reports, and thesis, contributing to the efficiency and comprehensiveness of the study.

The rest of this paper is organized as follows. In Section II, the method process is described in detail. In Section III, we describe the challenges of IRSs and our mapping study. In Section IV, the results and future directions are discussed. Finally, in Section V, the conclusion is presented.

## II. METHOD PROCESS

This paper presents an SMS for IRSs. This process is divided into three main stages: planning, conducting, and analyzing. The planning stage includes 4 phases, as shown in Fig. 1. In the following, we explain the details of the phases and strategies used in our proposed SMS. It should be noted that the proposed SMS in this study is written in the C# programming language and utilizes the JSON<sup>1</sup> data format.

<sup>1</sup>JavaScript Object Notation.

## A. PLANNING THE MAPPING STUDY

We begin the review process by defining the scope and research questions (RQs) that will guide our investigation. The next step is to establish a search strategy.

### 1) DEFINING THE RESEARCH QUESTIONS (RQ)

RQ is a critical first step in any review process as it helps to narrow the scope of a topic into a specific area of study. Finding a suitable answer to the RQ can facilitate progress in research. In this study, six distinct research questions have been proposed and are presented in Table 2, along with their motivation.

### 2) DETERMINE THE SEARCH STRATEGY

While most search methods rely on manual search and backward snowballing to identify related studies [11], our approach utilizes a web robot to automate the search process. Once the research scope is defined, the developed web robot automatically explores studies and information relevant to the research field, including papers published in journals, conferences, workshops, books, technical reports, and thesis which serves as our search space. The search process consists of four phases, illustrated in Fig. 1.

- **Phase 1:** In this phase, an initial set of primary studies is identified, including review studies and surveys collected through an expert's informal search, as presented in Table 1. From these studies, an initial set of keywords is extracted, and the expert may also add some keywords to this set.
- **Phase 2:** In this phase, the web robot searches for related studies in the Google Scholar environment using the keyword set as a reference. Google Scholar is chosen as a reference for extracting related studies in this study. After that, an expert reviews this set to identify related papers and eliminate unrelated ones based on the criteria in Table 3. Additionally, the cited papers from the primary studies set are added to the initial paper set as related studies. The result of this phase is a paper set that includes all the related studies in the research field.
- **Phase 3:** In this phase, the web robot extracts authors' information and search spaces (such as journals, conferences, workshops, etc.) for each related study from sources like Google Scholar and publisher websites. This information is utilized to address the RQs. However, due to constraints in the data extraction process, such as the unavailability of direct access to the reference site, there may be some missing values. To address this, an expert manually adds the missing values to the dataset. Additionally, the set of keywords is updated based on the keywords found in related studies.
- **Phase 4:** In this phase, after the data extraction, the results are analyzed by an expert to answer the research questions. In this step, the expert manually determines the type of response system and the specific network domain of the related studies. Then, these studies are

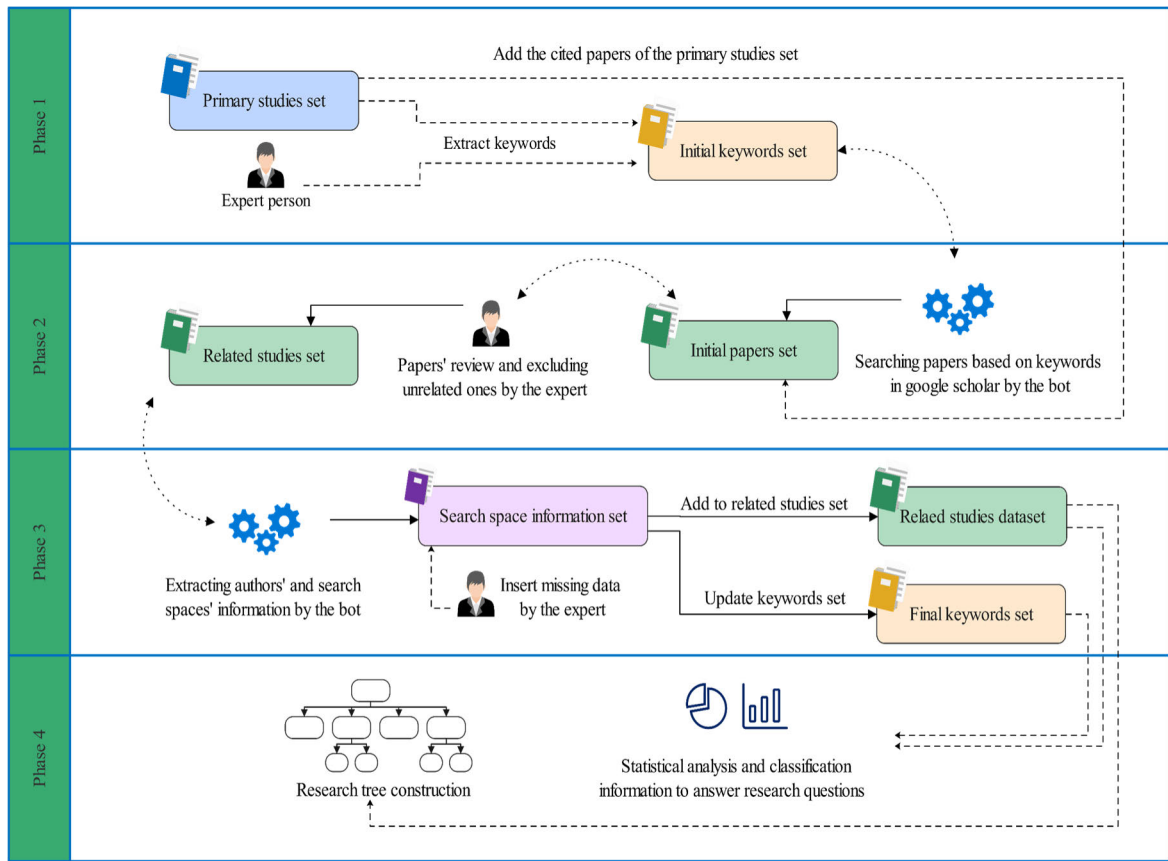


FIGURE 1. Method process.

TABLE 2. Research Questions (RQs).

No.	Research Question	Motivation
1	What is the annual publication rate of studies in this field (RQ1)?	Answering this question provides insights into the level of research community interest and attention towards the field of IRS over different time periods.
2	What are the research topics and network domains covered in the field of IRS (RQ2)?	By addressing this question, the researcher will be able to identify important topics within the field of IRS, explore the research landscape, identify specific network domains, and uncover emerging trends.
3	What are the primary keywords and terms associated with IRS (RQ3)?	By answering this question, the researcher gains insight into the prominent keywords and common phrases associated with IRS.
4	What are the differences between our SMS and the mentioned primary studies (RQ4)?	The researcher will identify the distinctions between our SMS and the primary studies (Table 1) or any other survey.
5	Which authors and researchers are active in this field (RQ5)?	The answer to this question assists researchers in identifying the leading authors in the field of study.
6	Which journals and conferences publish studies on IRS, and which publishers are considered the best in this field (RQ6)?	By answering this question, researchers can determine the top and most reputable journals, conferences, and publishers in the field of IRS based on commonly recognized criteria.

mapped to the research tree, which is described in detail in Section IV. The outcomes and statistical information of this phase can provide sufficient knowledge to effectively address the RQs.

### 3) DEFINITIONS

In this section, we will provide definitions to clarify our search strategy.

- **Defining the search space**

The search space includes journals, conferences, workshops, books, technical reports, and thesis. We add

survey studies (the primary studies set in Table 1) and their references to the initial papers set. The remaining search space is completed by the web robot during the search process (phase 2). The time interval for the search process is from 1996 to March 2023.

- **Specifying the search arrangement**

As mentioned earlier, our objective is to identify all studies in the field of IRS. To accomplish this, it is crucial to select the appropriate keywords. First, we extracted keywords from the primary studies set (Table 1) and added them to our keyword set. Furthermore, additional

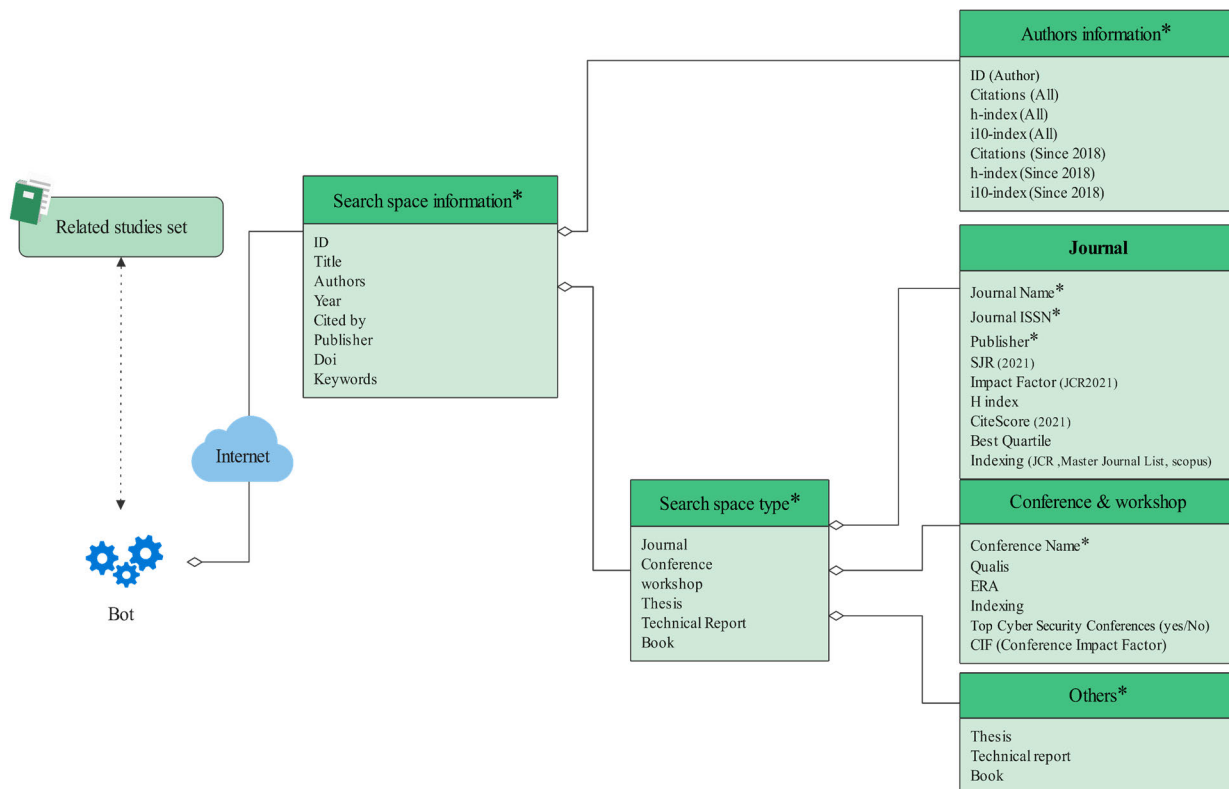


FIGURE 2. Search space information.

TABLE 3. Unrelated paper exclusion criterion.

ID	Exclusion Criterion
EC1	The study does not relate to IRS
EC2	The study does not relate to the sub-topics of the IRS
EC3	The study only relates to IDS
EC4	The study's language is not English
EC5	The study is not accessible

keywords were included in this set based on the expert’s opinion. Then, the keywords are sorted based on their importance to initiate the search process.

• **Determining the related studies**

Since manual searches to identify related studies are time-consuming, we have proposed a method that significantly reduces search time by using a web robot. The web robot employs the keyword set to find related studies.

However, to ensure the inclusion of only related studies and to eliminate unrelated ones caused by common keywords in other research fields, an expert carefully assesses the title, keywords, and abstract of each study. Consequently, unrelated studies are excluded from the initial papers set based on the exclusion criterion presented in Table 3. This approach aims to

TABLE 4. Search space exclusion rules.

Search space	ID	Exclusion rules
Journal	JER1	Not indexed in JCR, Master Journal List, and Scopus
	JER2	Best Quartile=Q4 or N/A
Conference	CER1	Qualis is N/A or Qualis<B3 (ERA is N/A or ERA=C)
Workshop	WER1	Qualis is N/A or Qualis<B3 (ERA is N/A or ERA=C)

enhance the accuracy and performance of our proposed method.

• **Determining high-quality search space**

The proposed SMS process first utilizes the web robot to obtain all search spaces to cover all research field studies. As high-quality studies are typically published in high-grade search spaces, we have defined rules for selecting these studies. We have considered various standard qualification metrics for each search space type, including SJR (SJR 2022), Impact Factor (JCR 2022), H index, CiteScore (2022), Best quartile for journals, and metrics such as Qualis (2012) and ERA (2010) for conferences and workshops. Table 4 shows the exclusion rules. Obviously, studies satisfied by these rules are discarded as low-quality studies. Due to the lack of appropriate criteria to determine the quality level of the thesis, technical report, and book, we focused solely on journals and conference papers.

**TABLE 5.** Sample unrelated studies.

No	Title	Year	Reason of exclusion
76	Intrusion detection: A survey	2005	EC3
124	A survey on MANET intrusion detection	2007	EC3
110	Rollbackable automated intrusion response system	2004	EC4
369	Active Response System in Anomalous Intrusion Detection on Android	2012	EC2
758	Cost-based adaptive intrusion response system	2007	EC5
1650	Comprehensive comparative-genomic analysis of type 2 toxin-antitoxin systems and related mobile stress response systems in prokaryotes	2009	EC1

#### 4) DATA EXTRACTION

Data extraction is performed in phase 3, where the web robot collects valuable data from multiple sources, including publishers' websites, Google Scholar, Scopus, Scimagojr.com, and Conferenceranks.com. Due to limitations in accessing certain resources, the web robot only extracts the starred information in Fig. 2, and the remaining information is completed by the expert.

#### B. CONDUCTING THE MAPPING STUDY

According to the definitions and strategies of the SMS process, the web robot found 6143 non-duplicate studies based on the initial keyword set. Subsequently, the expert excluded unrelated studies using the criteria presented in Table 3. As a result, 287 papers remained as related studies. Table 5 shows a sample of unrelated studies along with the reasons for their exclusion. For instance, Study 76th lacks contributions to intrusion response and focuses solely on intrusion detection, leading to its exclusion based on the EC3 criterion in Table 3. Furthermore, Tables 6 and 7 a sample of journals, conferences, and workshops that were discarded based on the exclusion rules specified in Table 4. Table 8 shows the number of related studies based on their search space type. Lastly, after selecting the related studies and extracting the necessary information, we have compiled a set of related studies along with useful information for further analysis.

#### C. ANALYZING THE MAPPING STUDY

Following the data extraction process, the results are analyzed and discussed to address the research questions. One of the objectives of this study is to distinguish between different types of IRS. To achieve this, it is necessary to identify different types of response systems. Several taxonomies for response systems have been proposed, as shown in Table 1. For instance, Curtis et al. proposed a taxonomy of IRS in six dimensions, including attack timing, type of attack, type of attacker, degree of suspension, attack implications, and environmental

constraints [2]. Stakhanova et al. and Shamel-Send et al. They have proposed another classification of IRSs, which includes the following criteria [7], [10]:

- **Level of automation:** an IRS can be divided into three categories as notification, manual, or automated system. *Notification systems:* Notification systems in IRS refer to the mechanisms that inform system administrators about potential or ongoing security incidents in a computer network. These systems can be triggered by different types of events, such as intrusion detection alerts or system logs that indicate unusual activity. Notification systems can use different methods to deliver alerts, such as emails, SMS messages, or instant messaging applications. The information of an alert includes the description of the attack, source and destination IP, and user account [7], [12].

*Manual response systems:* In these systems, which have a higher level than notification systems, there is a set of pre-defined responses. Based on the type of attack, the administrator applies responses that have a greater effect on reducing the damage to the network. For example, can include actions such as isolating affected systems or blocking network traffic. The issue mentioned in these systems is the delay between intrusion and the admin's response.

*Automatic response systems:* Automatic response systems refer to the set of actions that are triggered automatically in response to a security incident in a computer network. These systems are designed to reduce the response time to security incidents and minimize the potential damage caused by a security breach. The challenges raised in these systems are choosing an inappropriate response and ensuring that the response is sufficient to deal with the attack.

- **Adjustment ability:**
  - Static (Non-adaptive):* The response selection in these systems does not change over time. In fact, there is no mechanism in these systems to evaluate The effectiveness of applying these responses in dealing with intrusions.
  - Adaptive:* In this approach, the system has the ability to automatically adjust the appropriate responses and the order of applying them based on the response history.
- **Response time:**
  - Delayed:* In delayed mode, responses are applied after an intrusion is detected. Most existing IRS use this approach, but this approach has weak security compared to the proactive approach due to the delay in applying the response. Because there is a possibility that an attack can cause serious damage to the network before detection and response.
  - Proactive (preemptive):* On the other hand, the aim of proactive approach predict intrusion and prevent Possible damage to network resources. In general, it is difficult to implement and guarantee 100% correctness of prediction.

**TABLE 6.** Sample extracted journal search spaces and results of the journal selection.

No.	Journal name	ISSN	Publisher	Indexing			Best quartile	Exclusion rules
				JCR	Master journal list	Scopus		
7	Journal of Systems Engineering and Electronics	1004-4132	IEEE	✓	✓	N/A	Q4	JER2
21	Information Sciences	0020-0255	springer	✓	✓	✓	Q1	–
12	International Journal of Engineering and Technical Research (IJETR)	2321-0869	-	N/A	N/A	N/A	N/A	JER1
34	Journal of Information Security and Applications	2214-2126	Elsevier	✓	✓	✓	Q2	–

**TABLE 7.** Sample extracted conference and workshop search spaces and their selection results.

No.	Conference & workshop name	Qualis	ERA	Indexing	Exclusion rules
5	IFIP International Information Security Conference	B1	B	springer	–
20	International Conference on Machine Learning and Cybernetics	B4	C	IEEE	CER1
93	Annual Workshop on Cyber Security and Information Intelligence Research	N/A	N/A	ACM	WER1
7	Annual Computer Security Applications Conference	A1	A	IEEE	–

**TABLE 8.** Related studies type based on Search spaces.

No.	Study type	Number
1	Journal	99
2	Conference	132
3	Workshop	18
4	Thesis	24
5	Book	9
6	Technical report	5

- **Cooperating ability:**

*Autonomous:* These systems identify and manage intrusions independently, for example, if a HIDS detects an intrusion on a host, a local response is triggered on that host.

*Cooperative:* These systems include a set of IRS and are able to work cooperatively against intrusion. These systems are more complex than autonomous systems and require strong coordination between their components.

- **Response selection:**

*Static mapping:* These systems have a simple construction, but their responses are predictable for attackers, making them vulnerable to attacks, especially DoS attacks.

*Dynamic mapping:* The response selection mechanism in these systems is based on parameters such as confidence, frequency, and intensity of the attack. Responses may vary depending on the type of attack target and are selected in real-time based on the attack's characteristics.

*Cost-sensitive mapping:* These systems consider a trade-off between attack damage and response cost, taking into account parameters such as attack type, attack target, and response cost. However, accurately measuring these parameters can be a challenge in the design of these systems.

- **The activity of triggered response:**

*Passive:* Passive response systems do not prevent attacks or reduce the attack damage and only provide information about the attack.

*Active:* Active system's purpose is to reduce the attack's damage. In addition, these systems seek to harm the attacker.

- **Applying location:**

Most IRSs apply responses to the attacked host or attacker's machine. If suitable locations in the network are identified, the response cost can be reduced. The variety of responses in different locations provides a more effective framework for IRS systems, as its behavior will be less predictable. Extracting the "attack path" can help to identify suitable locations [10].

Table 9 presents an overview of the strengths and weaknesses of different types of IRSs. Our research tree, as shown in Fig. 3, is derived from these classifications. We have added another category to the response systems called "Specific Attacks" because, in the investigation of related studies, some response systems are specifically designed for certain types of attacks. After evaluating the title, abstract, or reading the full text, we determine the type of response system and the domain network of study. Subsequently, the studies are mapped in the research tree. If a study includes several types of response systems, we choose the topic that contributes the most to the study as its main topic. After describing the search process and the obtained results, the RQs presented in Table 2 are discussed.

### 1) WHAT IS THE ANNUAL PUBLICATION RATE OF STUDIES IN THIS FIELD (RQ1)?

Answering this question can help determine the level of attention the research community has given to the topic in different years within the time interval of our study (1996-2023). The

TABLE 9. Strengths and weaknesses of IRSs.

Type of level	IRS	Strengths	Weaknesses
Level of automation	Notification systems	<ul style="list-style-type: none"> <li>- Easy implementation</li> <li>- Timely notification</li> <li>- Automates alert generation</li> <li>- Scalability</li> <li>- Cost-effective</li> </ul>	<ul style="list-style-type: none"> <li>- False positives</li> <li>- Lack of response to the intrusion</li> <li>- Lack of detecting the severity of attacks</li> </ul>
	Manual response systems	<ul style="list-style-type: none"> <li>- Cost-effective</li> <li>- Easy implementation</li> </ul>	<ul style="list-style-type: none"> <li>- Delay in response time</li> <li>- Susceptible to human error</li> <li>- Limited scalability</li> </ul>
	Automatic response systems	<ul style="list-style-type: none"> <li>- Quick response time</li> <li>- Reduce human error</li> <li>- Continuous monitoring</li> </ul>	<ul style="list-style-type: none"> <li>- False positives</li> <li>- Costly implementation and maintenance</li> <li>- Limited flexibility</li> </ul>
Adjustment ability	Static (Non-adaptive)	<ul style="list-style-type: none"> <li>- Easy implementation</li> <li>- Cost-effective</li> </ul>	<ul style="list-style-type: none"> <li>- Unable to adapt to changing environments</li> <li>- Not effective against new or unknown attacks</li> <li>- No evaluation mechanism for response effectiveness</li> </ul>
	Adaptive	<ul style="list-style-type: none"> <li>- Effective against new or unknown attacks</li> <li>- Adaptive to changing environments</li> <li>- Ability to learn and improve response over time</li> </ul>	<ul style="list-style-type: none"> <li>- Costly implementation</li> <li>- Requires significant computational resources</li> </ul>
Response time	Delayed	<ul style="list-style-type: none"> <li>- Cost-effective</li> </ul>	<ul style="list-style-type: none"> <li>- Weak security</li> <li>- Delay in applying the response</li> <li>- Possibility of serious damage before applying response</li> </ul>
	Proactive (preemptive)	<ul style="list-style-type: none"> <li>- Taking preventive measures to stop attacks before of occur (Reducing the overall risk)</li> <li>- Costly implementation</li> </ul>	<ul style="list-style-type: none"> <li>- False positives</li> <li>- Requires continuous monitoring and updating for effectiveness</li> <li>- No guarantee of accurate prediction</li> </ul>
Cooperating ability	Autonomous	<ul style="list-style-type: none"> <li>- Operate independently without human intervention</li> </ul>	<ul style="list-style-type: none"> <li>- False positives</li> <li>- Applying the response locally</li> </ul>
	Cooperative	<ul style="list-style-type: none"> <li>- Include a set of IRS and are able to work cooperatively against intrusion</li> <li>- The distribution of workload among IRS systems</li> </ul>	<ul style="list-style-type: none"> <li>- Coordination between IRSs is complex to establish and maintain</li> <li>- Costly implementation and maintenance</li> </ul>
Response selection	Static mapping	<ul style="list-style-type: none"> <li>- Simple to implement and maintain</li> <li>- Effective against known attacks</li> </ul>	<ul style="list-style-type: none"> <li>- Inflexible and unable to adapt to new or unknown attacks</li> <li>- Limited effectiveness in complex attack scenarios</li> <li>- May not be scalable to large-scale IRS systems</li> </ul>
	Dynamic mapping	<ul style="list-style-type: none"> <li>- More flexible and adaptive response to new threats</li> <li>- Selecting the most appropriate response based on the specific situation</li> </ul>	<ul style="list-style-type: none"> <li>- Costly implementation and maintenance</li> <li>- Requires significant computational resources</li> <li>- Not always selecting the best response due to complex decision-making</li> </ul>
	Cost-sensitive mapping	<ul style="list-style-type: none"> <li>- Cost-effective decisions in selecting responses</li> </ul>	<ul style="list-style-type: none"> <li>- Accurate cost estimation is difficult</li> <li>- Requiring regular cost estimates over time</li> </ul>
The activity of triggered response	Passive	<ul style="list-style-type: none"> <li>- Lower cost and complexity compared to active systems</li> <li>- Provide valuable information about attack patterns and trends</li> </ul>	<ul style="list-style-type: none"> <li>- More prone to false positives</li> <li>- Require more expertise to operate and interpret their results effectively</li> </ul>
	Active	<ul style="list-style-type: none"> <li>- Quick response time</li> </ul>	<ul style="list-style-type: none"> <li>- Costly implementation and maintenance</li> <li>- False positives</li> <li>- False negatives</li> </ul>
Applying location	Static location	<ul style="list-style-type: none"> <li>- Easy implementation</li> </ul>	<ul style="list-style-type: none"> <li>- Predictability of system behavior for the attacker</li> </ul>
	Dynamic location	<ul style="list-style-type: none"> <li>- Applying response in suitable locations can reduce response cost</li> <li>- A variety of responses in different locations provides a more effective framework for IRS</li> <li>- The unpredictability of system behavior</li> </ul>	<ul style="list-style-type: none"> <li>- Identifying suitable locations in the network can be difficult</li> </ul>

number of publications for each year is shown in Fig. 4, which includes studies published until the end of March 2023. Based on the results, we divided the study period into Two time periods for further examination of IRSs.

- **1996-2010:** Simultaneously, with the increase of attacks on computer networks, security systems such as IDS

and IRS proposed to identify and deal with attacks. As observed in Fig. 5, the growth of published studies in the field of response systems has been increasing in these years. The highest number of published studies is between the years 2007 and 2010.

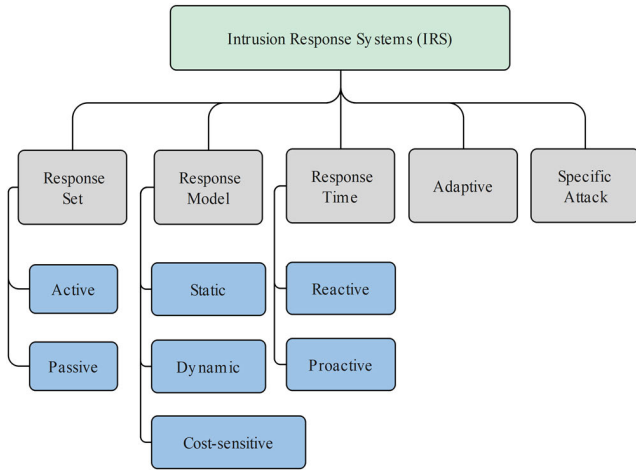


FIGURE 3. Research tree.

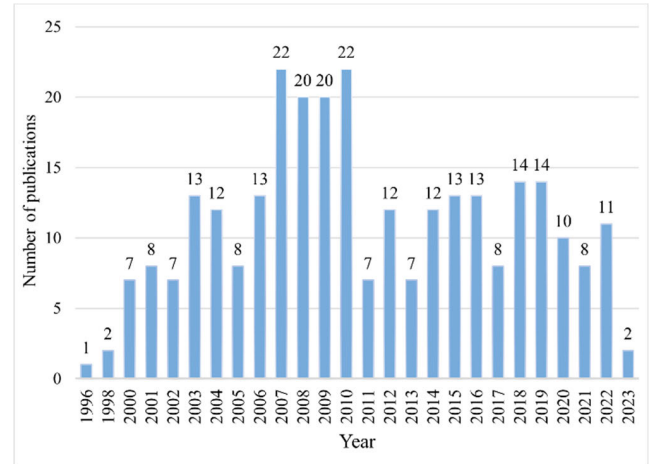


FIGURE 5. Evolution of IRS publications over time.

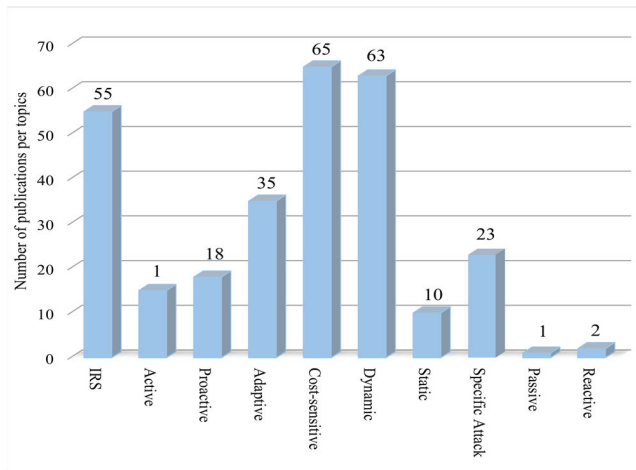


FIGURE 4. Number of publications per topic (Response model).

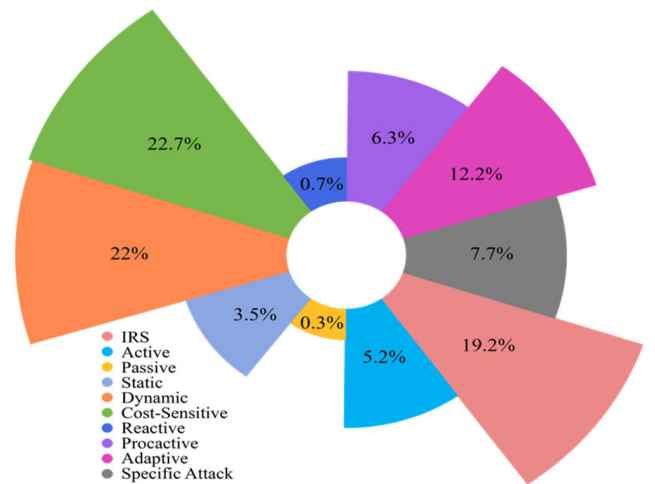


FIGURE 6. Percentage of publications per Topic (Response model).

- 2011-2023:** Due to the increase in network services, the volume of attacks on networks has also increased. Therefore, network administrators in organizations and companies need to respond to attacks in real-time to ensure uninterrupted network service delivery to users. As a result, a significant number of studies published in recent years focus on cost-sensitive and dynamic response models. However, the issues and challenges of IRSs are still not fully resolved, and there are open issues in this field. In Section IV, we will mention these items.

2) WHAT ARE THE RESEARCH TOPICS AND NETWORK DOMAINS COVERED IN THE FIELD OF IRS (RQ2)?

Obtaining knowledge of the research topics and scope is essential for researchers in a particular field. By answering this question, researchers can gain insights into the primary research topics within the field of IRS, the research tree, network domains, and emerging trends. This information allows researchers to understand the current landscape of the field and make informed decisions about their research directions.

In this study, the topics and network domains in the IRS field are presented separately in Fig. 5, 6, 7, and 8. Fig. 5 and 6 illustrate the number and percentage of publications on various topics or response models. For instance, dynamic, cost-sensitive, and adaptive models have garnered significant attention from researchers due to their effectiveness in addressing challenges arising from dynamic environments, cost considerations, and the need for adaptability. Some studies have focused on general and related topics in the field of IRS. These studies include surveys, taxonomies of response systems and attacks, defensive mechanisms, etc. We have organized them under the category of IRS for better understanding. Furthermore, Table 10 presents the response models of the related studies along with their references. After reviewing the studies, we have identified the specific networks for which response models have been proposed. Fig. 7 shows a visual representation that categorizes these networks. Furthermore, Fig. 8 presents the evolutionary progression of these networks in the field of IRS over time. This visual representation aids in comprehending the extent



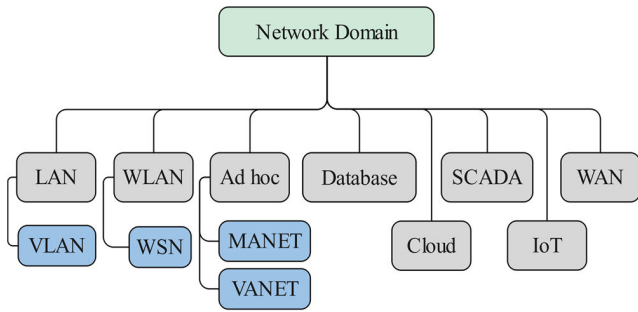


FIGURE 7. Specific network domain in the IRS field.

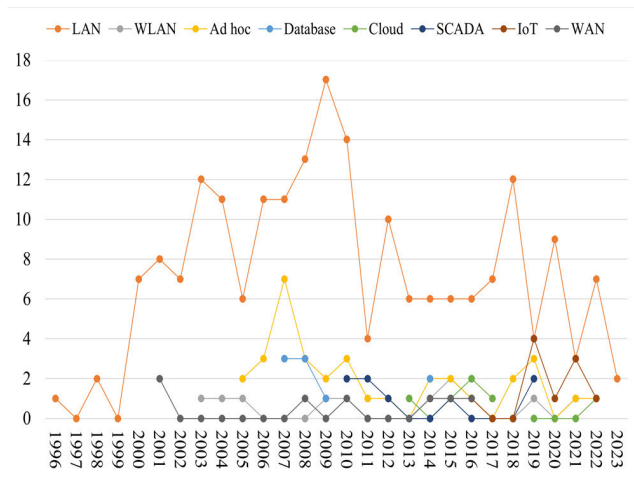


FIGURE 8. Evolution of the IRS network domain over time.

of researchers' attention and inclination toward proposing response models for various networks throughout the years.

As we can see in Fig. 8, it can be inferred that in recent years, emerging networks such as IoT have received more attention from researchers, in addition to LAN networks. For example, 10 out of 11 studies published in IoT networks were between 2019 and 2022. The number of studies published in various networks in the IRS field is presented in Table 11.

3) WHAT ARE THE PRIMARY KEYWORDS AND TERMS ASSOCIATED WITH IRS (RQ3)?

As mentioned in the third phase of the data extraction process (see Fig. 1), missing values are added to the dataset by the expert. One of the missing values may be the study's keywords. The study's keywords can be extracted directly from studies that contain an author's keywords section by the web robot or indirectly from studies that lack this section by the expert. The most frequent keywords are then selected based on a threshold value (five in this study). In this study, from 767 extracted keywords, 45 most frequent ones are chosen and shown in Table 12. Keywords can provide valuable insights. For instance, analyzing their frequency in relevant studies reveals that a considerable proportion of research has utilized graph theory to evaluate attacks (such as targets, vulnerabilities, and risk calculation). Furthermore,

TABLE 10. The response models of the related studies.

Response model	Ref
IRS	[6-10, 13-62]
Cost-sensitive	[1, 63-126]
Dynamic	[2, 5, 12, 127-186]
Static	[187-196]
Proactive	[197-214]
Reactive	[215, 216]
Active	[217-231]
Passive	[232]
Adaptive	[233-267]
Specific attack	[268-289]

TABLE 11. Studies published in various networks in the IRS field.

Specific domain	Num
LAN / VLAN	201 / 3
WLAN / WSN	8 / 3
Ad hoc / MANET / VANET	6 / 19 / 8
Database	9
Cloud	6
SCADA	8
IoT	11
WAN	5

a significant number of studies have employed the Markov Decision Process (MDP) to select the optimal response.

4) WHAT ARE THE DIFFERENCES BETWEEN OUR SMS AND THE MENTIONED PRIMARY STUDIES (RQ4)?

Our purpose of this RQ is to provide a comparison between our study and the primary studies. The closest review or survey paper to our study is shown in Table 1. Table 13 highlights the differences between these studies and our research. The primary studies have presented different categories for types of attacks, risk assessment, and types of response systems. In our study, response systems are categorized in a research tree. Additionally, we have investigated the evolution of IRSs and their network domains, which have not been mentioned in previous studies. Also, by analyzing the statistical information obtained, we discuss the trend and tendency of researchers to address issues in the IRS field in this study.

5) WHICH AUTHORS AND RESEARCHERS ARE ACTIVE IN THIS FIELD (RQ5)?

The answer to this question can help researchers identify the leading authors in the field of IRS. Among the 639 authors who have published studies in this field, we have identified 16 authors as active authors, each of whom has published at least 4 studies. Fig. 9 presents the authors with the highest

TABLE 12. Frequent keywords.

No.	Extracted keywords	Num	Synonym
1	Intrusion detection	67	Attack detection, Anomaly detection
2	Intrusion response	50	Incident response, Response policy, Attack response
3	Intrusion detection system	45	IDS
4	Intrusion response system	40	IRS
5	Automated intrusion response	28	Automated Intrusion Response System(AIRS), Automated response strategies, Automated intrusion response decision
6	Network Security	20	
7	Security	16	
8	Attack Graph	14	Attack trees, Attack path, Attack Response Tree (ART)
9	Markov decision process	13	MDP, POMDP, MDP modeling, Multiagent Markov decision processes, Markov decision process model, Markov decision process, Partially Observable Markov Decision Process(POMDP), Markov processes
10	Mobile Agent	12	
11	Countermeasures	12	
12	Response cost	11	
13	IDS	10	
14	Automated response	10	
15	Game theory	10	
16	Internet of Things	10	IoT
17	Intrusion	9	
18	Cost-sensitive	9	
19	DDoS attacks	9	
20	Response	9	
21	Computer Security	9	
22	Information security	8	
23	IRS	8	
24	Risk assessment	8	Risk management, Risk analysis
25	MANET	8	
26	Response system	8	
27	Ad-Hoc Networks	8	
28	Reinforcement learning	8	
29	Cyber security	8	
30	Active response	7	
31	Taxonomy	7	
32	Intrusion Detection and Response	6	
33	Decision making	6	
34	Security Policy	6	
35	SDN	6	Software-Defined Network
36	DoS attacks	6	
37	Fuzzy logic	5	
38	Attacks	5	
39	Countermeasure selection	5	
40	Intrusion prevention	5	
41	Intrusion containment	5	
42	WSN	5	
43	Risk management	5	
44	Security metrics	5	
45	Machine learning	5	ML

TABLE 13. Our study vs. Primary studies.

Ref.	Review type	Number of studies	Number of search spaces	Time interval	Category type	The evolution process	Open issues	Trend
[5]	No SMS	41	19	1996	Taxonomy	✗	✓	✗
[2]	No SMS	10	7	Up to 2000	Taxonomy	✗	✗	✗
[6]	No SMS	8	8	Up o 2006	Taxonomy	✗	✗	✗
[7]	No SMS	28	22	Up to 2007	Taxonomy	✗	✗	✗
[8]	No SMS	17	15	Up to 2012	Taxonomy	✗	✗	✗
[9]	No SMS	66	58	Up to 2012	Taxonomy	✓	✓	✗
[10]	No SMS	91	70	Up to 2014	Taxonomy	✓	✓	✗
Our study	SMS	287	202	Up to March 2023	Research tree	✓	✓	✓

TABLE 14. Author-level metrics.

Author	Number of studies	Cited By (IRS Studies)	h-index		i10-index		Citations		The latest published related study
			All	Sinds 2018	All	Sinds 2018	All	Sinds 2018	
Cuppens, Frédéric	14	477	45	19	178	53	10875	2127	2016
Cuppens-Boulahia, Nora	12	402	35	18	125	47	5186	1657	2016
Basu, Samik	8	564	29	12	74	21	2958	606	2013
Papadaki, Maria	8	122	27	22	45	34	2152	1267	2014
Stakhanova, Natalia	8	567	23	19	41	32	2778	1684	2012
Wong, Johnny S	8	564	-	-	-	-	-	-	2013
Debar, Herve	7	390	43	24	98	52	10448	2585	2018
Bagchi, Saurabh	6	348	57	38	178	123	10972	5046	2008
Foo, Bingrui	6	348	-	-	-	-	-	-	2008
Iannucci, Stefano	6	95	13	10	15	11	642	382	2022
Kanoun, Wael	6	160	11	9	13	9	362	212	2012
Shameli-Sendi, Alireza	6	398	16	14	22	17	1251	852	2018
Wu, Yu-Sung	6	348	-	-	-	-	-	-	2008
Strasburg, Chris	6	156	8	5	7	4	242	80	2013
Anuar, Nor Badrul	5	199	50	46	94	86	12758	10124	2017
Spafford, Eugene H	5	331	60	31	144	61	19711	2779	2008

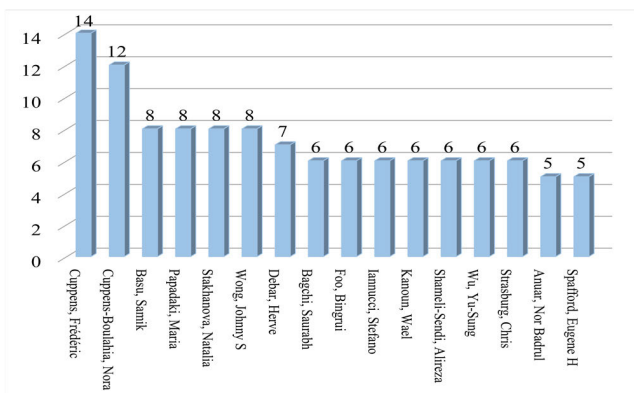


FIGURE 9. Authors active in the IRS field.

number of studies. Active authors are often evaluated based on various metrics, including the h-index, i10-index, and citation counts, to assess their research performance and impact.

TABLE 15. Search spaces set statistics.

No.	Study type	Number of Studies	Search spaces
1	Journal	99	74
2	Conference	132	113
3	Workshop	18	15

TABLE 16. High-quality search spaces.

No.	Study type	Search spaces
1	Journal	42
2	Conference	40
3	Workshop	3

The h-index measures an author’s productivity and citation impact, providing a balanced view of their scholarly output. The i10-index, on the other hand, focuses on the number of

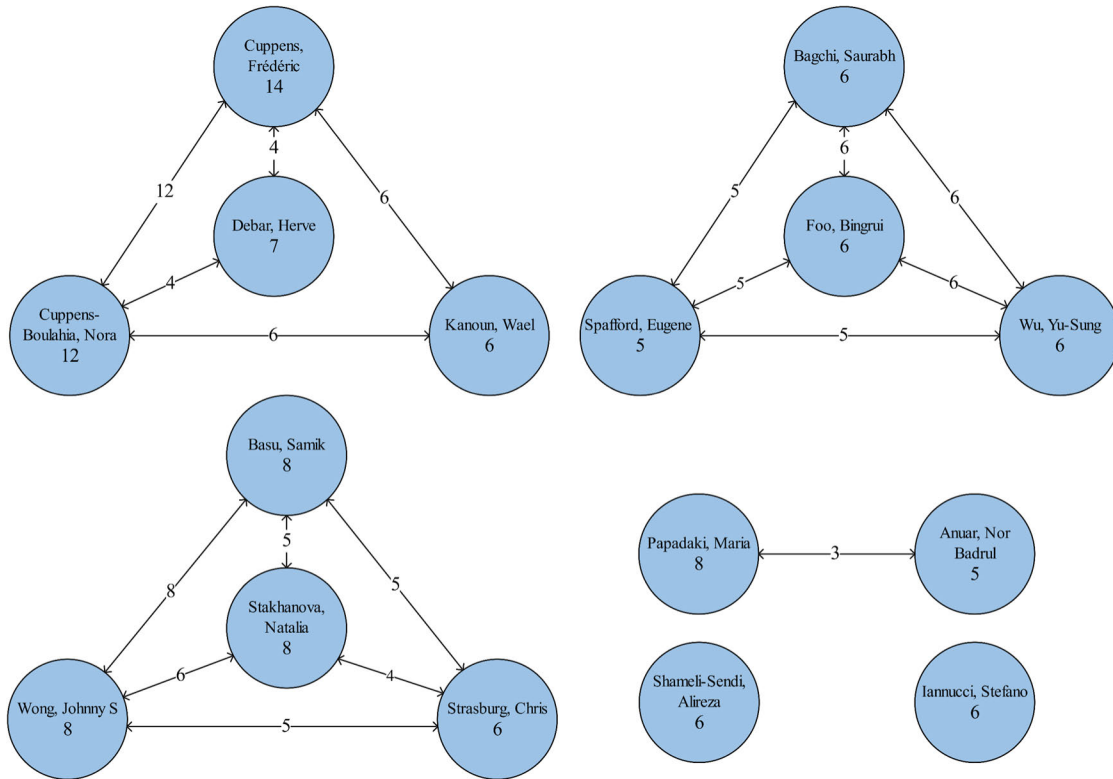


FIGURE 10. The shared studies were published among active authors.

publications by an author that has received at least 10 citations each, reflecting both productivity and impact.

By comparing these metrics among active authors, we can gain insights into their relative research impact and distinguish their contributions based on these quantitative indicators. Table 14 provides a comparison of these metrics. Additionally, Fig. 10 illustrates the shared studies published among active authors. The numbers on the edges indicate the number of shared studies.

### 6) WHICH JOURNALS AND CONFERENCES PUBLISH STUDIES ON IRS, AND WHICH PUBLISHERS ARE CONSIDERED THE BEST IN THIS FIELD (RQ6)?

This question aims to identify the top search spaces (journals, conferences, and workshops) that are pioneering and active in the field of IRS. This information can help researchers in identifying valid publications that are currently active in their research area. Based on the extracted information (see Table 8), we found that 99 studies have been published in 74 different journals. In addition, there were 132 conferences and 18 workshop studies that have been published in 113 and 15 different search spaces, respectively. Table 15 shows the statistical information of the search spaces.

Based on the defined criteria for identifying high-quality search spaces (see Table 4), 42 journal search spaces were selected as high-quality journals. Table 16 shows the number of search spaces that meet the defined criteria. We have

provided high-quality journals, conferences, and workshops in Tables 17, 18, and 19, respectively. Table 17 shows the information on reputable journals that have been ranked based on the JCR parameter (above 6). Tables 18 and 19 show the top conferences and workshops, respectively, determined by the ERA and Qualis parameters [290]. Other high-quality search spaces have been included in the Appendix section. Additionally, We identified the active search spaces that have published the highest number of studies over the years. These active search spaces are shown in Fig. 11 and 12.

### III. CHALLENGES OF OUR MAPPING STUDY AND IRSS

In this section, we present the challenges and advantages of our mapping studies in finding related studies in the research field. Additionally, we discuss the challenges faced by response systems in different networks.

#### A. CHALLENGES AND ADVANTAGES OF THE MAPPING STUDY

- **Challenges**

*Sensitivity to initial keyword selection:*The effectiveness of the proposed method relies on the choice of initial keywords. If inappropriate or inadequate keywords are selected for the research field, the search process may deviate and lead to inaccurate or incomplete results.

*Potential blocking by Google:*To ensure uninterrupted access to search results, the design and implementation

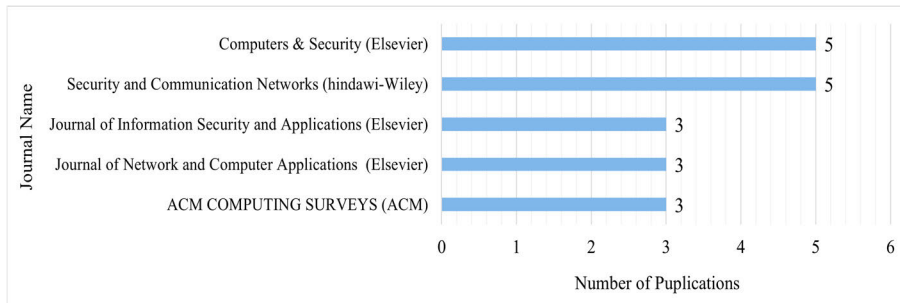


FIGURE 11. Active journals in the IRS field.

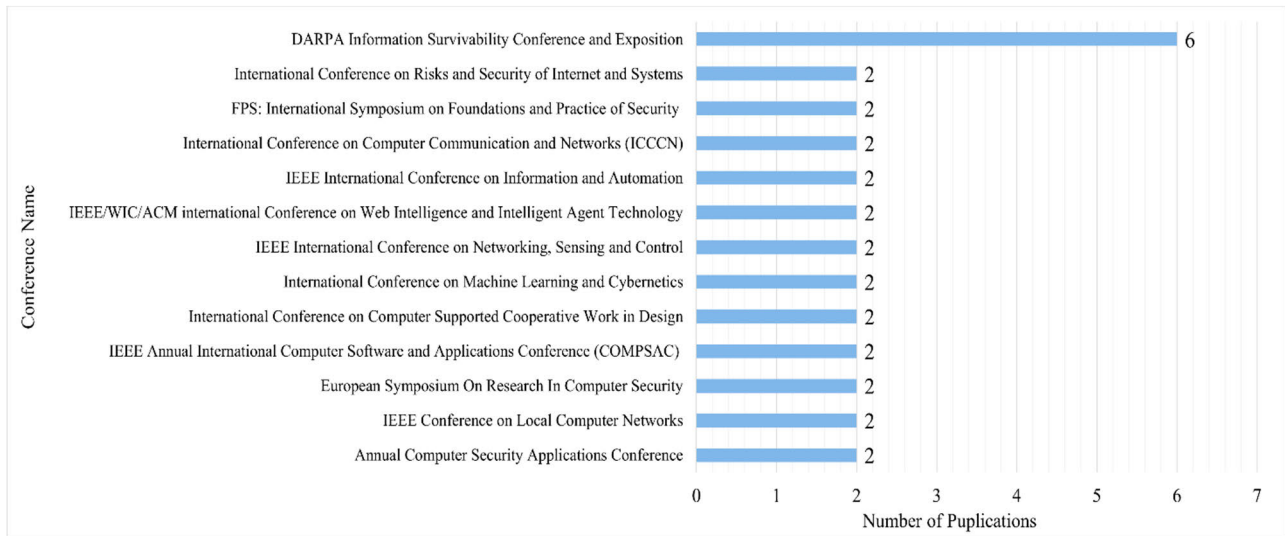


FIGURE 12. Active conferences in the IRS field.

TABLE 17. The best active journals in the IRS field.

No.	Journal name	Publisher	Journal ISSN	SJR (2022)	Impact Factor (JCR2022)	H Index	CiteScore (2022)	Best Quartile
1	IEEE Communications Surveys & Tutorials	IEEE	1553-877X	14.248	35.6	240	82.5	Q1
2	ACM COMPUTING SURVEYS	ACM	0360-0300	4.457	16.6	190	28.5	Q1
3	IEEE Transactions on Industrial Informatics	IEEE	1551-3203	4.002	12.3	170	22.4	Q1
4	IEEE Internet of Things Journal	IEEE	2327-4662	3.747	10.6	149	17.4	Q1
5	IEEE Transactions on Wireless Communications	IEEE	1536-1276	5.662	10.4	241	16.9	Q1
6	Journal of Network and Computer Applications	Elsevier	1084-8045	2.384	8.7	129	19	Q1
7	Expert Systems with Applications	Elsevier	0957-4174	1.873	8.5	249	12.6	Q1
8	Information Sciences	Elsevier	0020-0255	2.285	8.1	210	13.4	Q1
9	Journal of Management Information Systems	Taylor & Francis	0742-1222	3.064	7.7	161	10.7	Q1
10	Decision Support Systems	Elsevier	0167-9236	2.076	7.5	170	12.5	Q1
11	Future Generation Computer Systems	Elsevier	0167-739X	2.043	7.5	151	21.1	Q1
12	IEEE Transactions on Dependable and Secure Computing	IEEE	1545-5971	1.828	7.3	92	10.4	Q1

of the web robot should be carefully executed to prevent it from being blocked by Google or other search engines.

The proposed method has been designed to minimize the risk of being blocked by Google. Nevertheless, the web robot

is capable of resuming the search process from the point where it was blocked.

*Missing data:* Due to limitations in the web robot structure and restricted access to some resources, there is missing data

**TABLE 18. The best active conferences in the IRS field.**

No.	Name	Qualis	ERA	Indexing	Top Cyber Security Conferences (yes/No)	CIF(Conference Impact Factor)
1	Annual Computer Security Applications Conference	A1	A	IEEE	yes	1.97
2	European Symposium On Research In Computer Security	A2	A	Springer	yes	1.7
3	ACM Conference on Embedded Network Sensor Systems	A1	A	ACM	-	-
4	Annual Computer Security Conference	A1	A	Citeseer	-	-
5	IEEE Conference on Local Computer Networks	A2	A	IEEE	-	-
6	Symposium on Reliable Distributed Systems	A2	A	IEEE	-	-
7	International Conference on Dependable Systems and Networks (DSN)	A1	N/A	IEEE	-	-
8	International Joint Conference on Autonomous Agents and Multiagents Systems	A1	N/A	ACM	-	-
9	IEEE Annual International Computer Software and Applications Conference (COMPSAC)	A2	B	IEEE	-	-
10	IEEE Symposium on Computers and Communications(ISCC)	A2	B	IEEE	-	-
11	International Conference on Advanced Information Networking and Applications (AINA)	A2	B	IEEE	-	-
12	IEEE International Conference on Communications (ICC)	A2	B	IEEE	-	-
13	International Conference on Autonomic Computing (ICAC)	A2	B	IEEE	-	-
14	IEEE Wireless Communications and Networking Conference	A2	B	IEEE	-	-
15	Network Operations and Management Symposium	A2	B	IEEE	-	-

**TABLE 19. The best active workshops in the IRS field.**

No.	Name	Qualis	ERA	Indexing
1	IEEE Computer Security Foundations Workshop	A1	N/A	IEEE
2	Computer Security Foundations Symposium	N/A	A	IEEE
3	International Workshop on Recent Advances in Intrusion Detection	A2	B	Springer

in the data extraction process. The missing data is completed by the researcher or an expert.

• **Advantages**

*Time efficiency:* Compared to manual methods, our approach has demonstrated improved efficiency in terms of the time required to find relevant studies in the research field. The automated nature of the web robot allows for rapid extraction and compilation of relevant information, saving researchers time.

*Generalizability:* Our method can be generalized to various research fields, enabling researchers from different domains to utilize it for extracting related studies in their respective areas of research.

**B. CHALLENGES OF IRSS**

In recent years, significant research has been conducted on designing IRSs for various networks. However, developing an effective and efficient IRS is not without challenges. In this section, we explore and analyze these challenges in different networks. Generally, the challenges of an IRS can be summarized as follows:

*Detection accuracy:* Ensuring accurate detection of intrusions while minimizing false positives and false negatives, as it is crucial to distinguish genuine threats from benign activities.

*Scalability:* Ensuring that the response system can handle the increasing size and traffic of the network without compromising performance or response time.

*Heterogeneity:* Dealing with diverse network technologies, protocols, and devices, and ensuring compatibility and interoperability among them.

*Adaptability:* Adapting to evolving intrusion techniques and tactics employed by attackers to bypass detection and response mechanisms.

*Latency:* Minimizing the delay in response transmission across the network to ensure timely and efficient communication.

*Reliability:* Designing robust response systems that can withstand network failures, disruptions, or hardware/software malfunctions and maintain uninterrupted service.

*Quality of Service (QoS):* Balancing and optimizing response delivery in terms of latency, throughput, reliability, and other performance metrics based on network requirements.

*Resource constraints:* Managing limited resources, such as bandwidth, processing power, and memory, to provide efficient response services without exceeding the network’s capabilities.

*Dynamic network topology:* Adapting to changes in network topology due to device mobility, node failures, or network reconfiguration, and maintaining effective response mechanisms.

*Energy efficiency:* Designing response systems that minimize energy consumption, particularly in resource-constrained devices like the Internet of Things (IoT) devices or mobile networks.

*Privacy and trust:* Ensuring the privacy of user data and establishing trust in the response system, especially in scenarios involving sensitive or personal information.

However, each network has its own limitations and unique characteristics that need to be considered in designing a response system. In the following, we will discuss the important constraints and challenges of the main networks.

- **LAN networks:**

*Limited network visibility:* In addition to the above challenges in IRSs, LAN environments often have multiple segments or subnets, which can limit the visibility of network traffic. IRSs need to account for these segmented subnets. Limited network visibility within LAN environments can be addressed by deploying dedicated network monitoring tools. These tools provide enhanced visibility into network traffic, enabling IRSs to effectively select responses based on the overall network situation.

- **WAN networks:**

*Distributed WAN networks:* WAN networks often have longer latency compared to local networks, due to the geographical distance between network endpoints. This latency can impact the timeliness of intrusion detection and response. IRSs must account for network latency and optimize response mechanisms to minimize delays and ensure timely actions. On the other hand, Coordinating intrusion response activities across a distributed WAN network can be challenging. Establishing a centralized management system that can efficiently manage response actions across multiple locations is essential for effective intrusion response in the WAN network.

*Bandwidth limitation:* IRSs must consider bandwidth limitations in these networks and minimize data transmission and response execution.

- **WLAN/WSN networks:**

Some of the challenges in these networks include limited resources, scalability, real-time response, dynamic network topology, and privacy, as briefly mentioned above.

- **Cloud networks:**

*Shared responsibility model:* Cloud networks operate under a shared responsibility model, where the cloud service provider is responsible for the security of the underlying infrastructure, while the customer is responsible for securing their applications, data, and configurations within the cloud environment. Coordinating and aligning intrusion response efforts between the cloud

provider and the customer can be challenging due to differing responsibilities and levels of control.

*Network complexity:* Cloud networks are highly complex, consisting of various interconnected components, such as virtual machines, containers, load balancers, and network gateways. Designing IRSs that can effectively monitor and respond to threats across this intricate network architecture requires a comprehensive understanding of the cloud network topology and the ability to adapt to dynamic changes.

*Scalability:* Cloud networks are known for their scalability, allowing for the rapid provisioning and de-provisioning of resources based on demand. IRSs must be designed to scale seamlessly with the cloud environment to handle the increasing volume of network traffic and events while maintaining performance and response times.

*Multi-tenancy:* Cloud networks often serve multiple customers or tenants. IRSs need to be designed to operate effectively in a multi-tenant environment, ensuring that security incidents and responses are isolated and appropriate for each customer. Proper segregation of data and response activities is essential to maintain the security and privacy of each tenant.

*Compliance and legal considerations:* Cloud networks are subject to various compliance requirements and legal considerations. Designing IRSs that comply with relevant regulations and meet legal requirements is crucial. Incorporating proper auditing, logging, and incident reporting mechanisms is necessary to ensure compliance and support any legal investigations.

- **IoT networks:**

*Massive scale and heterogeneity:* IoT devices come from various manufacturers and may use different communication protocols and standards. Ensuring interoperability and compatibility between the IRS and diverse IoT devices can be a challenge.

*Securing and monitoring with limited resources:* Many IoT devices have limited processing power, memory, and energy resources. Designing intrusion response mechanisms that can operate within these resource constraints while effectively detecting and responding to intrusions is a challenge.

*Network protocols and communication pattern:* IoT devices utilize a variety of communication protocols, such as MQTT, CoAP, and Zigbee, each with its own characteristics and requirements. Developing intrusion response mechanisms that can understand and interact with multiple protocols is essential for effective detection and response.

*Ensuring privacy and data protection:* IoT networks often involve devices with varying security capabilities and trust levels. Ensuring secure communication between devices and the IRS, including encryption, authentication, and secure protocols, is essential to protect the integrity and confidentiality of data.

- **SCADA networks:**

*Legacy Infrastructure:* SCADA networks often consist of legacy systems with outdated technologies and protocols. These systems were not initially designed with security in mind, making it challenging to implement IRSs. Upgrading and securing legacy infrastructure without disrupting critical operations is a complex task.

*Interconnectivity:* SCADA networks are becoming more interconnected with enterprise networks and the internet for data exchange and remote access. This increased interconnectivity expands the attack surface and introduces vulnerabilities. Designing IRSs that can monitor and respond to threats across different network segments and interconnected systems requires careful planning and coordination.

*Real-time monitoring:* These networks often require real-time monitoring and response to ensure the timely detection and mitigation of security incidents. IRSs must be capable of monitoring network traffic, events, and anomalies in real-time, while also providing immediate and effective response actions. This requires efficient data collection, analysis, and response mechanisms.

*Resource limitations:* SCADA devices and systems typically have limited computational power, memory, and storage capabilities. Designing IRSs that can operate within these resource constraints while effectively detecting and responding to intrusions is a challenge. Optimizing the performance and efficiency of response mechanisms is crucial in SCADA networks.

*Regulatory compliance:* SCADA networks often operate in regulated industries, such as energy, water, and transportation. Designing and implementing IRSs that comply with industry-specific regulations and standards is essential. Meeting compliance requirements, such as data privacy, access controls, and incident reporting, can be challenging in SCADA environments.

- **Ad-hoc networks:**

Many characteristics of Ad-hoc networks, such as scalability, limited resources, and bandwidth constraints, are the same in WSN and IoT networks. However, the dynamic topology and decentralized nature are prominent features of Ad-hoc networks.

*Dynamic network topology:* Ad-hoc networks are characterized by their dynamic and self-organizing nature. Nodes in the network can join or leave at any time, causing frequent changes in the network topology. Designing IRSs that can adapt to these dynamic changes and effectively detect and respond to intrusions is a challenge.

*Lack of centralized authority:* Ad-hoc networks operate without a centralized authority or infrastructure. This decentralized nature makes it challenging to implement IRSs that rely on centralized control and monitoring. Designing distributed response mechanisms that can effectively coordinate and collaborate among nodes in the network is essential.

#### IV. DISCUSSIONS AND FUTURE DIRECTIONS

In the previous sections, the RQs have been addressed. The results can offer useful insights for researchers interested in the topic. In this section, we introduce emerging topics and networks in this research scope and outline potential future directions for improving response systems. As mentioned, our research has identified several studies that have proposed models of IRSs at different levels. Among these studies, some have employed reinforcement learning-based techniques for response selection [76], [144], [230], [249], [250], [255], [267], while others have utilized machine learning methods [44], [45], [51]. Additionally, certain approaches based on game theory [43], [65], [68], [73], [90], [122], [166], [186], [206], [209], [261], fuzzy logic [62], [80], [98], [102], [161], [174], genetic algorithms [30], [69], [70], hidden markov models [229], [247], markov decision processes [87], [142], [143], [145], [151], [276], partially observable Markov decision processes [124], [183], mobile agents [154], [181], [183], [203], [217], [231], [232], [271], [283], analytic hierarchy process [66], [178], [266], [275], and network quarantine channels [32], [33], [113] have been utilized to develop response models.

The distinction between reinforcement learning and machine learning is in their training approaches and decision-making processes. For instance, in reinforcement learning, the model interacts with the environment. In this approach, the model selects an optimal strategy by receiving rewards or penalties from the environment and generally does not require labeled training data. While in machine learning methods, (especially supervised learning), the model learns from labeled training data. Reinforcement learning methods, due to their ability to interact with dynamic and changing environments, exhibit more flexibility compared to machine learning methods. However, defining a reinforcement learning model in complex networks is a challenging task. Additionally, training reinforcement learning models typically demands significant computational resources. Game theory-based response models dynamically select the optimal response strategy by modeling the mutual behavior between defenders and attackers. However, these models usually require precise modeling of the complex interactions between defenders and attackers, leading to an increase in the implementation costs of the system. On the other hand, determining a suitable objective function for defenders and attackers in these methods is considered a challenge.

In issues involving uncertainty, fuzzy logic methods can be a suitable option for modeling and solving problems. The efficient use of these methods requires the precise adjustment of parameters and rules. In fuzzy logic, sensitivity to noisy data exists. Therefore, preprocessing is required to handle noisy data. Hidden Markov Models (HMM) and Markov Decision Processes (MDP) both play a role in solving decision-making problems, each with its own features and applications. HMM methods are utilized in pattern recognition, prediction, and the analysis of time sequences. On the



AQ:4 TABLE 20.

Number of Studies	Journal Name	Publisher	Journal ISSN	SJR (2022)	Impact Factor (JCR2022)	H Index	CiteScore (2022)	Best Quartile	Journal Country
2	IEEE Communications Surveys & Tutorials	IEEE	1553-877X	14.248	35.6	240	82.5	Q1	USA
3	ACM COMPUTING SURVEYS	ACM	0360-0300	4.457	16.6	190	28.5	Q1	USA
1	IEEE Transactions on Industrial Informatics	IEEE	1551-3203	4.002	12.3	170	22.4	Q1	USA
1	IEEE Internet of Things Journal	IEEE	2327-4662	3.747	10.6	149	17.4	Q1	USA
1	IEEE Transactions on Wireless Communications	IEEE	1536-1276	5.662	10.4	241	16.9	Q1	USA
3	Journal of Network and Computer Applications	Elsevier	1084-8045	2.384	8.7	129	19	Q1	ENGLAND
1	Expert Systems with Applications	Elsevier	0957-4174	1.873	8.5	249	12.6	Q1	ENGLAND
1	Information Sciences	Elsevier	0020-0255	2.285	8.1	210	13.4	Q1	USA
1	Journal of Management Information Systems	Taylor & Francis	0742-1222	3.064	7.7	161	10.7	Q1	ENGLAND
1	Decision Support Systems	Elsevier	0167-9236	2.076	7.5	170	12.5	Q1	NETHERLANDS
2	Future Generation Computer Systems	Elsevier	0167-739X	2.043	7.5	151	21.1	Q1	NETHERLANDS
2	IEEE Transactions on Dependable and Secure Computing	IEEE	1545-5971	1.828	7.3	92	10.4	Q1	USA
5	Computers & Security	Elsevier	0167-4048	1.605	5.6	112	11.1	Q1	ENGLAND
2	Computer Networks	Elsevier	1389-1286	1.625	5.6	150	10.7	Q1	NETHERLANDS
1	IEEE Transactions on Parallel and Distributed Systems	IEEE	1045-9219	1.89	5.3	153	9	Q1	USA
1	Computer Communications	Elsevier	0140-3664	1.395	6	118	11	Q1	NETHERLANDS
1	Frontiers of Computer Science	springer	2095-2228	0.786	4.2	42	6.2	Q1	CHINA
1	Journal in Computer Virology	springer	2263-8733	0.794	1.5	41	5.8	Q1	FRANCE
1	Annals of Nuclear Energy	Elsevier	0306-4549	0.859	1.9	77	3.6	Q1	ENGLAND
1	Journal of Systems Architecture	Elsevier	1383-7621	1.276	4.5	59	8.5	Q1	NETHERLANDS
2	IEEE Transactions on Network and Service Management	IEEE	1932-4537	1.693	5.3	65	7.6	Q1-Q2	USA
1	Ad Hoc Networks	Elsevier	1570-8705	1.301	4.8	104	12.1	Q1-Q2	NETHERLANDS
2	Computers & Electrical Engineering	Elsevier	0045-7906	0.95	4.3	84	7.1	Q1-Q2	ENGLAND
3	Journal of Information Security and Applications	Elsevier	2214-2126	1.279	5.6	54	9.7	Q1-Q2	NETHERLANDS
1	IEEE Access	IEEE	2169-3536	0.926	3.9	204	9	Q1-Q2	USA
1	Connection Science	Taylor & Francis	0954-0091	0.853	5.3	45	5.2	Q1-Q2	ENGLAND
1	Arabian Journal for Science and Engineering	springer	2191-4281	0.48	2.9	60	5.2	Q1-Q2	GERMANY
1	IEEE/ACM Transactions on Networking	IEEE	1063-6692	2.025	3.7	179	7.9	Q1-Q2	USA
2	Peer-to-Peer Networking and Applications	springer	1936-6442	0.865	4.2	42	6.9	Q2	USA
1	ACM Transactions on Autonomous and Adaptive Systems	ACM	1556-4665	0.487	2.7	44	4.6	Q2	USA
1	Journal of Computer Networks and Communications	Hindawi	2090-7141	0.713	2	29	8.9	Q2	ENGLAND
1	Algorithms	MDPI	1999-4893	0.497	2.3	46	3.7	Q2	SWITZERLAND
2	Journal of Computer Security	IOS Press	1875-8924	0.295	1.2	58	2.1	Q2	NETHERLANDS
1	Information & Computer Security	Emerald	2056-4961	0.47	1.4	55	3.7	Q2	ENGLAND
1	Cluster Computing	springer	1573-7543	0.618	4.4	63	7	Q2	USA
1	Computing	springer	1436-5057	0.824	3.7	64	6.4	Q2	AUSTRIA
1	SoftwareX	Elsevier	2352-7110	0.574	3.4	33	5.1	Q2	Netherlands
5	Security and Communication Networks	Hindawi-Wiley	1939-0114	0.494	1.968	58	2.6	Q2-Q3	ENGLAND
1	Mobile Information Systems	Hindawi	1574-017X	0.357	N/A	42	1.4	Q2-Q3	ENGLAND
1	Annales Des Télécommunications	springer	0003-4347	0.557	1.9	43	4.6	Q2-Q3	SWITZERLAND
1	Electronic Notes in Theoretical Computer Science	Elsevier	1571-0661	0.341	N/A	63	2	Q3	0
1	International Journal of Advanced Computer Science and Applications	SAI Organization	2156-5570	0.258	0.9	35	2.1	Q3	ENGLAND

TABLE 21.

Type	Number of studies	Name	Qualis	ERA	Indexing
C	1	International Conference on Dependable Systems and Networks (DSN)	A1	N/A	IEEE
C	2	Annual Computer Security Applications Conference	A1	A	IEEE
W	1	IEEE Computer Security Foundations Workshop	A1	N/A	IEEE
C	1	International Joint Conference on Autonomous Agents and Multiagents Systems	A1	N/A	ACM
C	1	ACM Conference on Embedded Network Sensor Systems	A1	A	ACM
C	1	Annual Computer Security Conference	A1	A	Citeseer
C	1	International Conference on Advanced Information Networking and Applications (AINA)	A2	B	IEEE
C	2	IEEE Conference on Local Computer Networks	A2	A	IEEE
C	2	European Symposium On Research In Computer Security	A2	A	springer
C	2	IEEE Annual International Computer Software and Applications Conference (COMPSAC)	A2	B	IEEE
C	1	IEEE International Conference on Communications	A2	B	IEEE
W	2	International Workshop on Recent Advances in Intrusion Detection	A2	B	springer
C	2	IEEE Symposium on Computers and Communications (ISCC)	A2	B	IEEE
C	2	Symposium on Reliable Distributed Systems	A2	A	IEEE
C	1	International Conference on Autonomic Computing (ICAC)	A2	B	IEEE
C	1	IEEE Wireless Communications and Networking Conference	A2	B	IEEE
C	1	International Conference on Computational Science	A2	A	springer
C	1	IEEE Symposium on Network Operations and Management	A2	B	IEEE
C	1	IFIP International Information Security Conference	B1	B	springer
C	1	International Conference on Networking	B1	N/A	springer
C	1	ACS/IEEE International Conference on Computer Systems and Applications	B1	C	IEEE
C	1	International Conference on Computer Science and Software Engineering	B1	N/A	IEEE
C	1	International Conference on Information Networking	B1	N/A	springer
C	1	IEEE Conference on Decision and Control	B1	A	IEEE
C	2	International Conference on Computer Communication and Networks (ICCCN)	B1	N/A	IEEE
C	1	International Conference on Networking (ICN)	B1	N/A	IEEE
C	1	International Conference on Computational Science and Its Applications	B1	N/A	springer
C	1	International Conference on Enterprise Information Systems, ICEIS	B1	C	scitepress
C	1	Euromicro International Conference on Parallel Distributed and Network-based Processing	B1	C	IEEE
C	1	International Asia-Pacific Web Conference	B2	N/A	springer
C	2	International Conference on Computer Supported Cooperative Work in Design	B2	B	IEEE
C	1	International Conference on Grid and Cooperative Computing	B2	C	springer
C	1	IEEE International Conference on Systems, Man and Cybernetics	B2	N/A	IEEE
C	1	IFIP International Conference on Distributed Applications and Interoperable Systems	B2	N/A	springer
C	1	International Conference on Security and Management	B3	N/A	academia
C	1	International Conference on Industrial Informatics (INDIN)	B3	N/A	IEEE
C	1	IEEE International Symposium on Dependable, Autonomic and Secure Computing	B3	N/A	IEEE
C	1	International Conference on Network and System Security	N/A	B	IEEE
C	1	Asia-Pacific Conference on Simulated Evolution and Learning	N/A	B	springer
C	1	ACM Symposium on Information, Computer and Communications Security	N/A	B	ACM
C	1	IEEE Conference on Industrial Electronics and Applications	N/A	A	IEEE
C	1	International Conference on Parallel and Distributed Computing, Applications and Technologies	N/A	B	IEEE
W	1	Computer Security Foundations Symposium	N/A	A	IEEE

other hand, MDP approaches focus on decision-making in dynamic environments. This model is typically employed for problems where the environment can be in various states at each moment, and an agent uses decision-making actions to improve its situation. The decision-making agent makes decisions based on a value function and an adoption strategy.

Challenges in HMM methods include sensitivity to high dimensions, managing uncertainty, and complexity in training. Significant challenges in using MDP methods include high temporal complexity (in solving problems with large state spaces) and the need for accurate knowledge of the environment.

However, the research conducted in this field is still not sufficiently effective, and there is a significant gap in designing an ideal and efficient IRS that can be used in real-world scenarios. The ability to effectively respond to intrusions requires solving a multi-objective decision-making problem that can simultaneously handle the mentioned challenges. These techniques consider the trade-offs between different objectives and generate a set of Pareto-optimal solutions, representing the best possible responses across the objectives. Therefore, one of the future directions is the design of IRS by solving multi-objective decision-making problems. In our opinion, other future directions that should be considered to improve the performance of IRS are summarized as follows.

Firstly, advancements in machine learning and artificial intelligence can significantly improve the accuracy and efficiency of attack detection algorithms. Leveraging these technologies can enable more precise identification of threats and reduce false positives. Additionally, the integration of response systems with threat intelligence platforms and security information and event management (SIEM) systems can provide a holistic view of network security. This integration allows for real-time monitoring, threat analysis, and better decision-making in incident response. According to the results of our SMS, IRSs have been developed for emerging networks such as the IoT in recent years [167], [216], [230], [261], [278], [285].

However, an examination of these studies indicates that IRSs in these networks are still in their early stages. With the proliferation of cloud computing and IoT devices, IRSs need to adapt and integrate seamlessly with these environments. Therefore, another future direction could be the development of specialized response mechanisms for these networks, taking into account their unique features and security challenges.

Furthermore, future response systems should emphasize adaptability and scalability to meet the evolving demands of network environments. As technology advances and new attack vectors emerge, response systems must be capable of adapting and incorporating innovative techniques to counter these threats effectively. In conclusion, the challenges faced by response systems in network environments are diverse and ever-evolving. Overcoming these challenges requires a multi-faceted approach that addresses performance, accuracy, fault tolerance, and future scalability. By embracing advancements in technology, integrating with threat intelligence platforms, and prioritizing adaptability, we can forge a path toward more robust and effective IRSs. From our point of view, in the context of IRSs, a Large Language Model (LLM) can play a crucial role in enhancing their effectiveness. The advantages of using an LLM are as follows:

*Threat intelligence:* LLMs can analyze vast amounts of security-related data, including threat intelligence feeds, security bulletins, and vulnerability databases. They can extract relevant information, identify patterns, and provide insights into emerging threats and attack techniques.

*Natural language understanding:* An LLM can help in understanding and processing natural language inputs from security analysts or users reporting potential security incidents. By understanding the intent and context of these inputs, the model can provide relevant guidance, suggestions, or automated responses.

*Threat hunting:* LLMs can assist security analysts in proactively searching for threats within the network. By analyzing network traffic, system logs, and other relevant data, the model can identify potential indicators of compromise, malicious behaviors, or unusual patterns that might indicate an ongoing attack.

*Intrusion response automation:* LLMs can automate various aspects of intrusion response processes. They can offer response templates or recommend actions by analyzing historical intrusion data. This can expedite response times, ensure consistent actions, and alleviate the workload on security analysts.

It's worth noting that the effectiveness of an LLM in an IRS relies on proper training, fine-tuning, and integration with other security tools and technologies. Moreover, privacy and data protection considerations should be taken into account when deploying such models in sensitive security environments.

Therefore, as future directions, we recommend the use and development of multi-objective decision-making techniques, integration of response systems with threat intelligence platforms and security information systems (SIEM), as well as the utilization of LLM. We believe these techniques can contribute to modeling an effective and efficient intrusion response system. Additionally, our analysis indicates that the development of intrusion response systems in emerging networks such as IoT can be considered an open issue.

## V. CONCLUSION

In this paper, we review the existing literature in the field of IRSs using a novel research methodology. To achieve this objective, we established several research questions to identify key issues, including the covered research topics and networks, active authors and search spaces, the number of publications in each topic, common keywords, and emerging trends. As a result, 287 related studies were identified during the study after applying the proposed semi-automated research methodology. Subsequently, a data extraction process was conducted on these studies to gather the necessary information for addressing the research questions. Based on the results, the IRS has garnered attention from researchers over the past two decades. Additionally, the findings indicate that emerging networks, such as IoT, have emerged as trending topics in this research field in recent years. We also examined the challenges and identified some future directions in response systems, which can serve as a research starting point for researchers interested in this field.

## APPENDIX HIGH-QUALITY JOURNALS

See the Table 20.

## HIGH-QUALITY CONFERENCES AND WORKSHOPS

See the Table 21.

## REFERENCES

- [1] M. Ghasemigol, H. Takabi, and A. Ghaemi-Bafghi, "A foresight model for intrusion response management," *Comput. Secur.*, vol. 62, pp. 73–94, Sep. 2016, doi: [10.1016/j.cose.2016.06.005](https://doi.org/10.1016/j.cose.2016.06.005).
- [2] C. A. Carver and U. W. Pooch, "An intrusion response taxonomy and its role in automatic intrusion response," in *Proc. IEEE Workshop Inf. Assurance Secur.*, West Point, NY, USA, Jun. 2000, pp. 129–135.
- [3] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. 12th Int. Conf. Eval. Assessment Softw. Eng. (EASE)*, Jun. 2008, pp. 1–10.
- [4] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.
- [5] E. A. Fisch, "Intrusion damage control and assessment: A taxonomy and implementation of automated responses to intrusive behavior," Ph.D. dissertation, Dept. Comput. Sci, Texas A&M Univ., College Station, TX, USA, 1996.
- [6] H. Wang, G. Wang, Y. Lan, K. Wang, and D. Liu, "A new automatic intrusion response taxonomy and its application," in *Proc. Int. Asia-Pacific Web Conf.*, Jan. 2006, pp. 999–1003.
- [7] N. Stakhanova, S. Basu, and J. Wong, "A taxonomy of intrusion response systems," *Int. J. Inf. Comput. Secur.*, vol. 1, nos. 1–2, p. 169, Feb. 2007, doi: [10.1504/ijics.2007.012248](https://doi.org/10.1504/ijics.2007.012248).
- [8] W. Kanoun, L. Samarji, N. Cuppens-Bouahia, S. Dubus, and F. Cuppens, "Towards a temporal response taxonomy," in *Proc. Int. Workshop Data Privacy Manage. (DPM)*, 2013, pp. 318–331.
- [9] A. Shameli-Sendi, N. Ezzati-Jivan, M. Jabbarifar, and M. Dagenais, "Intrusion response systems: Survey and taxonomy," *Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 1, pp. 1–14, Jan. 2012.
- [10] A. Shameli-Sendi, M. Cheriet, and A. Hamou-Lhadj, "Taxonomy of intrusion risk assessment and response system," *Comput. Secur.*, vol. 45, pp. 1–16, Sep. 2014, doi: [10.1016/j.cose.2014.04.009](https://doi.org/10.1016/j.cose.2014.04.009).
- [11] S. Jalali and C. Wohlin, "Systematic literature studies: Database searches vs. backward snowballing," in *Proc. ACM-IEEE Int. Symp. Empirical Softw. Eng. Meas.*, Sep. 2012, pp. 29–38.
- [12] D. J. Ragsdale, C. A. Carver, J. W. Humphries, and U. W. Pooch, "Adaptation techniques for intrusion detection and intrusion response systems," in *Proc. IEEE Int. Conf. Syst. Man Cybern.*, Nashville, TN, USA, Oct. 2000, pp. 2344–2349.
- [13] A. Adetoye, A. Choi, M. M. Arshad, and O. Soretire, "Network intrusion detection & response system," MSc DCNDS Group 4, Dept. Comput. Sci, Univ. College London, London, U.K., Tech. Rep., 2003. [Online]. Available: <http://www-icbocn.cs.ucl.ac.uk/teaching/ncs/group-reports/2003/2003-hailes-b.pdf>
- [14] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Comput. s.*, vol. 54, no. 1, pp. 1–37, Mar. 2021, doi: [10.1145/3431233](https://doi.org/10.1145/3431233).
- [15] N. B. Anuar, S. Furnell, M. Papadaki, and N. Clarke, "Response mechanisms for intrusion response systems (IRSS)," in *Proc. 5th Collaborative Res. Symp. Secur., E-Learning, Internet Netw.*, Plymouth, U.K., 2009, pp. 3–14. [Online]. Available: <https://citeseerx.ist.psu.edu/pdf/3351b55af45cf8e25ff9a999bafd3a9f6713691d>
- [16] N. B. Anuar, M. Papadaki, S. Furnell, and N. Clarke, "An investigation and survey of response options for intrusion response systems (IRSSs)," in *Proc. Inf. Secur. South Africa*, Aug. 2010, pp. 1–8.
- [17] S. Anwar, J. M. Zain, M. F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang, "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 39, Mar. 2017, doi: [10.3390/a10020039](https://doi.org/10.3390/a10020039).
- [18] S. Anwar, J. M. Zain, M. F. Zolkipli, Z. Inayat, A. N. Jabir, and J. B. Odili, "Response option for attacks detected by intrusion detection system," in *Proc. 4th Int. Conf. Softw. Eng. Comput. Syst. (ICSECS)*, Kuantan, Malaysia, Aug. 2015, pp. 195–200. [Online]. Available: [https://www.academia.edu/download/52249877/Response\\_option\\_for\\_attacks\\_detected\\_by\\_Intrusion\\_Detection\\_System.pdf](https://www.academia.edu/download/52249877/Response_option_for_attacks_detected_by_Intrusion_Detection_System.pdf)
- [19] A. Asosheh and N. Ramezani, "A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification," *WSEAS Trans. Comput.*, vol. 7, no. 4, pp. 281–290, 2008.
- [20] R. Brackney, "Cyber-intrusion response," in *Proc. 17th IEEE Symp. Reliable Distrib. Syst.*, West Lafayette, IN, USA, Oct. 1998, pp. 413–415.
- [21] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020, doi: [10.1109/COMST.2019.2953364](https://doi.org/10.1109/COMST.2019.2953364).
- [22] A. Carlin, M. Hammoudeh, and O. Aldabbas, "Intrusion detection and countermeasure of virtual cloud systems—State of the art and current challenges," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 6, pp. 1–15, 2015.
- [23] P. K. Chouhan, A. Beard, and L. Chen, "Intrusion response systems: Past, present and future," 2023, [arXiv:2303.03070](https://arxiv.org/abs/2303.03070).
- [24] P. F. da Silva and C. B. Westphall, "Improvements in the model for interoperability of intrusion detection responses compatible with the IDWG model," *Int. J. Netw. Manage.*, vol. 17, no. 4, pp. 287–294, Jul. 2007, doi: [10.1002/nem.626](https://doi.org/10.1002/nem.626).
- [25] P. E. Eng and M. Haug, "Automatic response to intrusion detection," M.S. thesis, Dept. Eng. Sci., Agder Univ. College, Grimstad, Norway, 2004.
- [26] B. A. Fessi, M. Hamdi, S. Benabdallah, and N. Boudriga, "Automated intrusion response system: Surveys and analysis," in *Proc. Int. Comput. Secur. Manage. (SAM)*, 2008, pp. 149–155. [Online]. Available: <https://www.academia.edu/4233060>
- [27] B. Foo, M. W. Glause, G. M. Howard, Y.-S. Wu, S. Bagchi, and E. H. Spafford, "Intrusion response systems: A survey," in *Proc. Inf. Assurance, Dependability Secur. Networked Syst.*, vol. 13, 2008, pp. 377–412.
- [28] A. A. Ghorbani, W. Lu, M. Tavallae, A. A. Ghorbani, W. Lu, and M. Tavallae, *Network Intrusion Detection and Prevention: Concepts and Techniques*. New York, NY, USA: Springer, 2010.
- [29] P. Gulihar and B. B. Gupta, "Cooperative mechanisms for defending distributed denial of service (DDoS) attacks," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, B. Gupta, D. P. Agrawal, D. Gupta and G. M. Perez, Eds. Cham, Switzerland: Springer, 2020, pp. 421–443.
- [30] Y. Guo, H. Zhang, Z. Li, F. Li, L. Fang, L. Yin, and J. Cao, "Decision-making for intrusion response: Which, where, in what order, and how long?" in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6.
- [31] M. Hamad, M. Tsantekidis, and V. Prevelakis, "Intrusion response system for vehicles: Challenges and vision," in *Proc. Int. Conf. Smart Cities Green ICT Syst.*, 2021, pp. 321–341.
- [32] E. Hooper, "An intelligent intrusion detection and response system using network quarantine channels: Adaptive policies and alert filters," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Intell. Agent Technol. Workshops*, Dec. 2006, pp. 45–48.
- [33] E. Hooper, "An intelligent intrusion detection and response system using network quarantine channels: Firewalls and packet filters," in *Proc. Int. Conf. Multimedia Ubiquitous Eng. (MUE)*, Apr. 2007, pp. 1193–1198.
- [34] Y.-A. Huang, "Intrusion detection and response systems for mobile ad hoc networks," Ph.D. dissertation, Dept. Comput. Sci., Univ. Georgia, Athens, GA, USA, 2006.
- [35] T. M. A.-K. Ibrahim, "Improving intrusion prevention, detection and response," Ph.D. dissertation, Dept. Sci. Technol., Univ. Plymouth, Plymouth, U.K., 2011.
- [36] Z. Inayat, A. Gani, N. B. Anuar, S. Anwar, and M. K. Khan, "Cloud-based intrusion detection and response system: Open research issues, and solutions," *Arabian J. Sci. Eng.*, vol. 42, no. 2, pp. 399–423, Jan. 2017, doi: [10.1007/s13369-016-2400-3](https://doi.org/10.1007/s13369-016-2400-3).
- [37] Z. Inayat, A. Gani, N. B. Anuar, M. K. Khan, and S. Anwar, "Intrusion response systems: Foundations, design, and challenges," *J. Netw. Comput. Appl.*, vol. 62, pp. 53–74, Feb. 2016, doi: [10.1016/j.jnca.2015.12.006](https://doi.org/10.1016/j.jnca.2015.12.006).
- [38] M. Jahnke, C. Thul, and P. Martini, "Comparison and improvement of metrics for selecting intrusion response measures against DoS attacks," in *Proc. GI Sicherheit Conf.*, Apr. 2008, pp. 382–393. [Online]. Available: <https://www.marko-jahnke.de/docs/work/sicherheit08.pdf>
- [39] P. Kabiri and A. A. Ghorbani, "Research on intrusion detection and response: A survey," *Int. J. Netw. Secur.*, vol. 1, no. 2, pp. 84–102, 2005.

- [40] M. Kaur, D. Lindskog, and P. Zavarovsky, "Integrating intrusion response functionality into the MANET specific dynamic intrusion detection hierarchy architecture," in *Proc. 9th Int. Conf. Ad Hoc Netw.*, 2018, pp. 69–80.
- [41] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures," 2019, *arXiv:1903.01541*.
- [42] A. Keshariya and N. Foukia, "DDoS defense mechanisms: A new taxonomy," in *Proc. Int. Workshop Data Privacy Manag.*, 2010, pp. 222–236.
- [43] C. Kiennert, Z. Ismail, H. Debar, and J. Leneutre, "A survey on game-theoretic approaches for intrusion detection and response optimization," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–31, Aug. 2018, doi: [10.1145/3232848](https://doi.org/10.1145/3232848).
- [44] A. Lopes, "Using machine learning to guide automated intrusion response," M.S. thesis, Dept. Comput. Sci., Cape Town Univ., Cape Town, South Africa, 2020.
- [45] A. Lopes and A. Hutchison, "Experimenting with machine learning in automated intrusion response," in *Proc. Int. Symp. Intell. Distrib. Comput.*, 2020, pp. 505–514.
- [46] S. Maschino, "Intrusion detection and response to automated attacks," in *Proc. 7th Int. Conf. Enterprise Inf. Syst. (ICEIS)*, 2005, pp. 522–525. [Online]. Available: <https://www.scitepress.org/PublishedPapers/2005/25408>
- [47] M. S. Mirpurayan, T. Tavizi, and H. Gharraee, "A comprehensive network intrusion detection and prevention system architecture," in *Proc. 6th Int. Symp. Telecommun. (IST)*, Tehran, Iran, Nov. 2012, pp. 954–958.
- [48] C. Mu, B. Shuai, and H. Liu, "Analysis of response factors in intrusion response decision-making," in *Proc. 3rd Int. Joint Conf. Comput. Sci. Optim.*, vol. 2, May 2010, pp. 395–399.
- [49] P. Nespoli, F. G. Mármol, and J. M. Vidal, "Battling against cyberattacks: Towards pre-standardization of countermeasures," *Cluster Comput.*, vol. 24, no. 1, pp. 57–81, Mar. 2021, doi: [10.1007/s10586-020-03198-9](https://doi.org/10.1007/s10586-020-03198-9).
- [50] P. Nespoli, D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1361–1396, 2nd Quart., 2018, doi: [10.1109/COMST.2017.781126](https://doi.org/10.1109/COMST.2017.781126).
- [51] R. Oliveira, B. Bhargava, M. Azarmi, E. Ferreira, W. Wang, and M. Lindermann, "Developing attack defense ideas for ad hoc wireless networks," in *Proc. 2nd Int. Workshop Dependable Netw. Comput. Mobile Syst. (DNCMS)*, New York, NY, USA, 2009, pp. 1–7. [Online]. Available: <https://www.cs.purdue.edu/homes/bb>
- [52] M. Papadaki, "Classifying and responding to network intrusions," Ph.D. dissertation, Dept. Sci. Technol., Plymouth Univ., Plymouth, U.K., 2004.
- [53] M. Papadaki, S. Furnell, B. Lines, and P. Reynolds, "Operational characteristics of an automated intrusion response system," in *Proc. IFIP Int. Conf. Commun. Multimedia Secur.*, 2003, pp. 65–75.
- [54] M. Papadaki and S. M. Furnell, "Informing the decision process in an automated intrusion response system," *Inf. Secur. Tech. Rep.*, vol. 10, no. 3, pp. 150–161, Jan. 2005, doi: [10.1016/j.istr.2005.07.002](https://doi.org/10.1016/j.istr.2005.07.002).
- [55] M. Papadaki, S. M. Furnell, S. Lee, B. Lines, and P. L. Reynolds, "Enhancing response in intrusion detection systems," *J. Inf. Warfare*, vol. 2, no. 1, pp. 90–102, 2003.
- [56] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, Jan. 2013, doi: [10.1016/j.jnca.2012.08.007](https://doi.org/10.1016/j.jnca.2012.08.007).
- [57] T. Rasha and S. Vincent, "A survey on intrusion response mechanism for MANET routing attacks," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 10, pp. 479–485, Oct. 2012.
- [58] N. Stakhanova, Y. Li, and A. A. Ghorbani, "Classification and discovery of rule misconfigurations in intrusion detection and response devices," in *Proc. World Congr. Privacy, Secur., Trust Manage. E-Bus.*, Aug. 2009, pp. 29–37.
- [59] Z. Wu, Y. Ou, and Y. Liu, "A taxonomy of network and computer attacks based on responses," in *Proc. Int. Conf. Inf. Technol., Comput. Eng. Manage. Sci.*, Nanjing, China, Sep. 2011, pp. 26–29.
- [60] O. Yousuf and R. N. Mir, "A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 292–323, Jun. 2019, doi: [10.1108/ics-07-2018-0084](https://doi.org/10.1108/ics-07-2018-0084).
- [61] W. T. Yue and M. Cakanyildirim, "Intrusion prevention in information systems: Reactive and proactive responses," *J. Manage. Inf. Syst.*, vol. 24, no. 1, pp. 329–353, Jul. 2007, doi: [10.2753/mis0742-1222240110](https://doi.org/10.2753/mis0742-1222240110).
- [62] M. Zaghoud and M. S. Al-Kahtani, "Contextual fuzzy cognitive map for intrusion response system," *Int. J. Comput. Inf. Technol.*, vol. 2, no. 3, pp. 471–478, 2013.
- [63] J. Baayer, B. Regragui, and A. Baayer, "False positive responses optimization for intrusion detection system," *J. Inf. Secur.*, vol. 5, no. 2, pp. 19–36, 2014, doi: [10.4236/jis.2014.52003](https://doi.org/10.4236/jis.2014.52003).
- [64] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt, "Using specification-based intrusion detection for automated response," in *Proc. 6th Int. Symp. Recent Adv. Intrusion Detection*, Pittsburgh, PA, USA, 2003, pp. 136–154.
- [65] M. Bloem, T. Alpcan, and T. Basar, "Intrusion response as a resource allocation problem," in *Proc. 45th IEEE Conf. Decis. Control*, San Diego, CA, USA, Dec. 2006, pp. 6283–6288.
- [66] B. Caskurlu, A. Gehani, C. C. Bilgin, and K. Subramani, "Analytical models for risk-based intrusion response," *Comput. Netw.*, vol. 57, no. 10, pp. 2181–2192, Jul. 2013, doi: [10.1016/j.comnet.2013.03.012](https://doi.org/10.1016/j.comnet.2013.03.012).
- [67] Z. Chen, H. Yong, and T. Zhao, "The research and implementation of incident response information system," presented at the Softw. Eng. Knowl. Eng., Theory Pract., Jan. 2012.
- [68] S. Du, X. Li, J. Du, and H. Zhu, "An attack-and-defence game for security assessment in vehicular ad hoc networks," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 215–228, Sep. 2014, doi: [10.1007/s12083-012-0127-9](https://doi.org/10.1007/s12083-012-0127-9).
- [69] B. A. Fessi, S. Benabdallah, N. Boudriga, and M. Hamdi, "A multi-attribute decision model for intrusion response system," *Inf. Sci.*, vol. 270, pp. 237–254, Jun. 2014, doi: [10.1016/j.ins.2014.02.139](https://doi.org/10.1016/j.ins.2014.02.139).
- [70] B. A. Fessi, S. Benabdallah, M. Hamdi, and N. Boudriga, "A new genetic algorithm approach for intrusion response system in computer networks," in *Proc. IEEE Symp. Comput. Commun.*, Sousse, Tunisia, Jul. 2009, pp. 342–347.
- [71] G. Gonzalez-Granadillo, J. Garcia-Alfaro, E. Alvarez, M. El-Barbori, and H. Debar, "Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index," *Comput. Electr. Eng.*, vol. 47, pp. 13–34, Oct. 2015, doi: [10.1016/j.compeleceng.2015.07.023](https://doi.org/10.1016/j.compeleceng.2015.07.023).
- [72] K. Haslum, A. Abraham, and S. Knapskog, "DIPS: A framework for distributed intrusion prediction and prevention using hidden Markov models and online fuzzy risk assessment," in *Proc. 3rd Int. Symp. Inf. Assurance Secur.*, Manchester, U.K., Aug. 2007, pp. 183–190.
- [73] W. He, C. Xia, H. Wang, C. Zhang, and Y. Ji, "A game theoretical attack-defense model oriented to network security risk assessment," in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, vol. 6, Wuhan, China, Dec. 2008, pp. 498–504.
- [74] N. Herold, M. Wachs, S.-A. Posselt, and G. Carle, "An optimal metric-aware response selection strategy for intrusion response systems," in *Proc. Int. Symp. Found. Pract. Secur.*, 2017, pp. 68–84.
- [75] T. Hussain, A. Beard, L. Chen, C. Nugent, J. Liu, and A. Moore, "From machine learning based intrusion detection to cost sensitive intrusion response," in *Proc. 6th Int. Conf. Cryptography, Secur. Privacy (CSP)*, Tianjin, China, Jan. 2022, pp. 124–130.
- [76] S. Iannucci, O. D. Barba, V. Cardellini, and I. Banicescu, "A performance evaluation of deep reinforcement learning for model-based intrusion response," in *Proc. IEEE 4th Int. Workshops Found. Appl. Self Syst.*, Umea, Sweden, Jun. 2019, pp. 158–163.
- [77] A. J. Ikuomola and A. S. Sodiya, "A credible cost-sensitive model for intrusion response selection," in *Proc. 4th Int. Conf. Comput. Aspects Social Netw. (CASoN)*, Sao Carlos, Brazil, Nov. 2012, pp. 222–227.
- [78] A. J. Ikuomola, A. S. Sodiya, A. T. Akinwale, and D. O. Aborisade, "An improved cost-sensitive intrusion response model," *J. Inf. Assurance Secur.*, vol. 8, no. 3, pp. 147–155, 2013.
- [79] A. J. Ikuomola, A. S. Sodiya, and J. O. Nehinbe, "A framework for collaborative, adaptive and cost sensitive intrusion response system," in *Proc. 2nd Comput. Sci. Electron. Eng. Conf. (CEEC)*, Sep. 2010, pp. 1–4.
- [80] D. Irugu, P. Balaji, and P. Nirupama, "FIRE: Fuzzy-logic based theoretic intrusion response and recovery engine," *Int. J. Comput. Sci. Trends Technol.*, vol. 3, no. 4, pp. 55–59, 2015.
- [81] M. Jahneke, C. Thul, and P. Martini, "Graph based metrics for intrusion response measures in computer networks," in *Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN)*, Oct. 2007, pp. 1035–1042.

- [82] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, and S. Dubus, "Risk-aware framework for activating and deactivating policy-based response," in *Proc. 4th Int. Conf. Netw. Syst. Secur.*, Sep. 2010, pp. 207–215.
- [83] C. Katar and A. Badreddine, "New multi-objective approach for dynamic risk-driven intrusion responses," *Frontiers Comput. Sci.*, vol. 14, no. 1, pp. 230–232, Feb. 2020, doi: [10.1007/s11704-019-8175-4](https://doi.org/10.1007/s11704-019-8175-4).
- [84] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, and H. Debar, "A service dependency model for cost-sensitive intrusion response," in *Proc. Eur. Symp. Res. Comput. Secur.*, Sep. 2010, pp. 626–642.
- [85] H. A. Kholidy, A. Erradi, S. Abdelwahed, and F. Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system," *Computing*, vol. 98, no. 11, pp. 1111–1135, Jun. 2016, doi: [10.1007/s00607-016-0495-8](https://doi.org/10.1007/s00607-016-0495-8).
- [86] S. K. Nejat and P. Kabiri, "An adaptive and cost-based intrusion response system," *Cybern. Syst.*, vol. 48, nos. 6–7, pp. 495–509, Jul. 2017, doi: [10.1080/01969722.2017.1319693](https://doi.org/10.1080/01969722.2017.1319693).
- [87] O. P. Kreidl, "Analysis of a Markov decision process model for intrusion tolerance," in *Proc. Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Chicago, IL, USA, Jun. 2010, pp. 156–161.
- [88] W. Lee, W. Fan, M. Miller, S. J. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response," *J. Comput. Secur.*, vol. 10, nos. 1–2, pp. 5–22, Jan. 2002, doi: [10.3233/jcs-2002-101-202](https://doi.org/10.3233/jcs-2002-101-202).
- [89] F. Li, Y. Li, Z. Yang, Y. Guo, L. Yin, and Z. Wang, "Selecting combined countermeasures for multi-attack paths in intrusion response system," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Hangzhou, China, Jul. 2018, pp. 1–9.
- [90] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, "A game theory based risk and impact analysis method for intrusion defense systems," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl.*, Rabat, Morocco, May 2009, pp. 975–982.
- [91] L. Mechtri, F. D. Tolba, and S. Ghanemi, "An optimized intrusion response system for MANET: An attack-severity aware approach," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 3, pp. 602–618, May 2018, doi: [10.1007/s12083-017-0573-5](https://doi.org/10.1007/s12083-017-0573-5).
- [92] C. Mu and Y. Li, "An intrusion response decision-making model based on hierarchical task network planning," *Expert Syst. Appl.*, vol. 37, no. 3, pp. 2465–2472, Mar. 2010, doi: [10.1016/j.eswa.2009.07.079](https://doi.org/10.1016/j.eswa.2009.07.079).
- [93] M. Papadaki and S. M. Furnell, "Achieving automated intrusion response: A prototype implementation," *Inf. Manage. Comput. Secur.*, vol. 14, no. 3, pp. 235–251, May 2006, doi: [10.1108/09685220610670396](https://doi.org/10.1108/09685220610670396).
- [94] A. Roy, D. S. Kim, and K. S. Trivedi, "Cyber security analysis using attack countermeasure trees," in *Proc. 6th Annu. Workshop Cyber Secur. Inf. Intell. Res.*, Apr. 2010, pp. 1–4.
- [95] A. Roy, D. S. Kim, and K. S. Trivedi, "Attack countermeasure trees (ACT): Towards unifying the constructs of attack and defense trees," *Secur. Commun. Netw.*, vol. 5, no. 8, pp. 929–943, Aug. 2012, doi: [10.1002/sec.299](https://doi.org/10.1002/sec.299).
- [96] L. Rui and L. Wanbo, "Intrusion response model based on AIS," in *Proc. Int. Forum Inf. Technol. Appl.*, vol. 1, Kunming, China, Jul. 2010, pp. 86–90.
- [97] D. Schnackenberg, K. Djahandari, and D. Sterne, "Infrastructure for intrusion detection and response," in *Proc. DARPA Inf. Survivability Conf. Expo.*, Hilton Head, SC, USA, Jan. 2000, pp. 3–11.
- [98] A. Shameli-Sendi and M. Dagenais, "ORCEF: Online response cost evaluation framework for intrusion response system," *J. Netw. Comput. Appl.*, vol. 55, pp. 89–107, Sep. 2015, doi: [10.1016/j.jnca.2015.05.004](https://doi.org/10.1016/j.jnca.2015.05.004).
- [99] A. Shameli-Sendi, M. Dagenais, and L. Wang, "Realtime intrusion risk assessment model based on attack and service dependency graphs," *Comput. Commun.*, vol. 116, pp. 253–272, Jan. 2018, doi: [10.1016/j.comcom.2017.12.003](https://doi.org/10.1016/j.comcom.2017.12.003).
- [100] Z. Shijie, Q. Zhiguang, L. Xucheng, Z. Xianfeng, Z. Feng, and L. Jinde, "Cost-based intelligent intrusion detection and response: Design and implement," in *Proc. 4th Int. Conf. Parallel Distrib. Comput., Appl. Technol.*, Chengdu, China, Aug. 2003, pp. 166–170.
- [101] D. K. Singh and P. Kaushik, "Analysis of decision making factors for automated intrusion response system (AIRS): A review," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 6, p. 471, Jan. 2016.
- [102] D. K. Singh and P. Kaushik, "Intrusion response prioritization based on fuzzy ELECTRE multiple criteria decision making technique," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102359, doi: [10.1016/j.jisa.2019.102359](https://doi.org/10.1016/j.jisa.2019.102359).
- [103] N. Stakhanova, "A framework for adaptive, cost-sensitive intrusion detection and response system," Ph.D. dissertation, Dept. Comput. Sci., Iowa State Univ., Ames, IA, USA, 2007.
- [104] N. Stakhanova, S. Basu, and J. Wong, "A cost-sensitive model for preemptive intrusion response systems," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Niagara Falls, ON, Canada, May 2007, pp. 428–435.
- [105] N. Stakhanova, C. Strasburg, S. Basu, and J. S. Wong, "Towards cost-sensitive assessment of intrusion response selection," *J. Comput. Secur.*, vol. 20, nos. 2–3, pp. 169–198, Jun. 2012, doi: [10.3233/jcs-2011-0436](https://doi.org/10.3233/jcs-2011-0436).
- [106] O. Stan, R. Bitton, M. Ezretz, M. Dadon, M. Inokuchi, Y. Ohta, T. Yagyu, Y. Elovici, and A. Shabtai, "Heuristic approach for countermeasure selection using attack graphs," in *Proc. IEEE 34th Comput. Secur. Found. Symp. (CSF)*, Dubrovnik, Croatia, Jun. 2021, pp. 1–16.
- [107] F. P. Stanley, "Intrusion detection and response for system and network attacks," M.S. thesis, Dept. Comput. Sci., Iowa State Univ., Ames, IA, USA, 2009.
- [108] C. Strasburg, N. Stakhanova, S. Basu, and J. S. Wong, "A framework for cost sensitive assessment of intrusion response selection," in *Proc. 33rd Annu. IEEE Int. Comput. Softw. Appl. Conf.*, vol. 1, Seattle, WA, USA, Jul. 2009, pp. 355–360.
- [109] C. Strasburg, N. Stakhanova, S. Basu, and J. S. Wong, "Intrusion response cost assessment methodology," in *Proc. 4th Int. Symp. Inf., Comput., Commun. Secur.*, Mar. 2009, pp. 388–391.
- [110] C. Strasburg, N. Stakhanova, J. Wong, and S. Basu, "The methodology for evaluating response cost for intrusion response systems," Dept. Comput. Sci., Iowa Univ., Ames, IA, USA, Tech. Rep. 199, 2008.
- [111] C. R. Strasburg, "A framework for cost-sensitive automated selection of intrusion response," M.S. thesis, Dept. Comput. Sci., Iowa State Univ., Ames, IA, USA, 2009.
- [112] M. Sun and Y. Guo, "The research on enhanced cost-based auto intrusion response decision," in *Proc. 5th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Beijing, China, Sep. 2009, pp. 1–4.
- [113] Y. Sun and R. Zhang, "Automatic intrusion response system based on aggregation and cost," in *Proc. Int. Conf. Inf. Autom.*, Jun. 2008, pp. 1783–1786.
- [114] S. Tanachaiwiwat, K. Hwang, and Y. Chen, "Adaptive intrusion response to minimize risk over multiple network attacks," *ACM Trans. Inf. Syst. Secur.*, vol. 19, pp. 95–96, Aug. 2002.
- [115] T. Toth and C. Kruegel, "Evaluating the impact of automated intrusion response mechanisms," in *Proc. 18th Annu. Comput. Secur. Appl. Conf.*, Las Vegas, NV, USA, Dec. 2002, pp. 301–310.
- [116] E. A. Toyin, I. A. Gbolahan, A. C. Bunmi, O. A. Patrick, and A. B. Aina, "Cost minimization model for an adaptive intrusion response system," *Indian J. Comput. Sci. Eng.*, vol. 3, no. 2, pp. 240–248, May 2012.
- [117] J. Wang, "Loss-sensitive decision rules for intrusion detection and response," Ph.D. dissertation, Dept. Comput. Inf. Sci., Pennsylvania Univ., Philadelphia, PA, USA, 2004.
- [118] S.-H. Wang, "Distributed and cooperative intrusion response models for mobile ad hoc networks," Ph.D. dissertation, Dept. Comput. Sci., California Univ., Davis, CA, USA, 2008.
- [119] S.-H. Wang, C. H. Tseng, K. Levitt, and M. Bishop, "Cost-sensitive intrusion responses for mobile ad hoc networks," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*, Sep. 2007, pp. 127–145.
- [120] H. Wei, D. Frinck, O. Carter, and C. Ritter, "Cost-benefit analysis for network intrusion detection systems," in *Proc. CSI 28th Annu. Comput. Secur. Conf.*, Mar. 2001, pp. 29–31.
- [121] Y. Wu and S. Liu, "A cost-sensitive method for distributed intrusion response," in *Proc. 12th Int. Conf. Comput. Supported Cooperat. Work Design*, Xi'an, China, Apr. 2008, pp. 760–764.
- [122] T. Yarygina and C. Otterstad, "A game of microservices: Automated intrusion response," in *Proc. IFIP Int. Conf. Distrib. Appl. Interoperable Syst.*, Jun. 2018, pp. 169–177.
- [123] W. T. Yue and M. Çakanyıldırım, "A cost-based analysis of intrusion detection system configuration under active or passive response," *Decis. Support Syst.*, vol. 50, no. 1, pp. 21–31, Dec. 2010, doi: [10.1016/j.dss.2010.06.001](https://doi.org/10.1016/j.dss.2010.06.001).
- [124] X. Zan, F. Gao, J. Han, X. Liu, and J. Zhou, "A hierarchical and factored POMDP based automated intrusion response framework," in *Proc. 2nd Int. Conf. Softw. Technol. Eng.*, San Juan, PR, USA, Oct. 2010, pp. 410–414.

- [125] Z. Zhang, P.-H. Ho, and L. He, "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach," *Comput. Secur.*, vol. 28, no. 7, pp. 605–614, Oct. 2009, doi: [10.1016/j.cose.2009.03.005](https://doi.org/10.1016/j.cose.2009.03.005).
- [126] M. Zhou and G. Yao, "Improved cost-sensitive model of intrusion response system based on clustering," in *Proc. Int. Conf. Electric, Commun. Autom. Control*, New York, NY, USA, Nov. 2012, pp. 931–937.
- [127] S. Alampalayam, "Intrusion detection and response model for mobile ad hoc networks," Ph.D. dissertation, Dept. Comput. Eng. Comput. Sci., Louisville Univ., Louisville, KY, USA, 2007.
- [128] A. Alazab, M. Hobbs, J. Abawajy, A. Khraisat, and M. Alazab, "Using response action with intelligent intrusion detection and prevention system against Web application malware," *Inf. Manage. Comput. Secur.*, vol. 22, no. 5, pp. 431–449, Nov. 2014, doi: [10.1108/imcs-02-2013-0007](https://doi.org/10.1108/imcs-02-2013-0007).
- [129] N. B. Anuar, M. Papadaki, S. Furnell, and N. Clarke, "A response selection model for intrusion response systems: Response strategy model (RSM)," *Secur. Commun. Netw.*, vol. 7, no. 11, pp. 1831–1848, Nov. 2014, doi: [10.1002/sec.896](https://doi.org/10.1002/sec.896).
- [130] T. Bouyahia, F. Autrel, N. Cuppens-Boulahia, and F. Cuppens, "Context aware intrusion response based on argumentation logic," in *Proc. 10th Int. Conf. Risk Secur. Internet Syst.*, Jul. 2016, pp. 91–106.
- [131] T. Bouyahia, N. Cuppens-Boulahia, F. Cuppens, and F. Autrel, "Multi-criteria recommender approach for supporting intrusion response system," in *Proc. Int. Symp. Found. Pract. Secur.*, Québec City, QC, Canada, Oct. 2017, pp. 51–67.
- [132] H. Debar, Y. Thomas, F. Cuppens, and N. Cuppens-Boulahia, "Enabling automated threat response through the use of a dynamic security policy," *J. Comput. Virol.*, vol. 3, no. 3, pp. 195–210, Mar. 2007, doi: [10.1007/s11416-007-0039-z](https://doi.org/10.1007/s11416-007-0039-z).
- [133] H. Debar, Y. Thomas, F. Cuppens, and N. Cuppens-Boulahia, "Response: Bridging the link between intrusion detection alerts and security policies," in *Intrusion Detection Systems*, vol. 38. Boston, MA, USA: Springer, 2008, ch. 6, pp. 129–170.
- [134] E. Doynikova and I. Kottenko, "Countermeasure selection based on the attack and service dependency graphs for security incident management," in *Proc. 10th Int. Conf. Risk Secur. Internet Syst.*, Jul. 2016, pp. 107–124.
- [135] T. Eom, J. B. Hong, S. An, J. S. Park, and D. S. Kim, "A framework for real-time intrusion response in software defined networking using pre-computed graphical security models," *Secur. Commun. Netw.*, vol. 2020, pp. 1–15, Feb. 2020, doi: [10.1155/2020/7235043](https://doi.org/10.1155/2020/7235043).
- [136] S. Fenet and S. Hassas, "A distributed intrusion detection and response system based on mobile autonomous agents using social insects communication paradigm," *Electron. Notes Theor. Comput. Sci.*, vol. 63, pp. 41–58, May 2002, doi: [10.1016/s1571-0661\(04\)80336-0](https://doi.org/10.1016/s1571-0661(04)80336-0).
- [137] A. Gabillon, Q. Z. Sheng, W. Mansoor, F. Cuppens, N. Cuppens-Boulahia, and W. Kanoun, "A formal framework to specify and deploy reaction policies," in *Web-Based Information Technologies and Distributed Systems*, vol. 2, 1st ed. Amsterdam, The Netherlands: Atlantis Press, 2010, ch. 8, pp. 159–188.
- [138] A. Gehani, "Support for automated passive host-based intrusion response," Ph.D. dissertation, Dept. Comput. Sci, Duke Univ., Durham, NC, USA, 2003.
- [139] G. Gonzalez-Granadillo, S. Dubus, A. Motzek, J. Garcia-Alfaro, E. Alvarez, M. Merialdo, S. Papillon, and H. Debar, "Dynamic risk management response system to handle cyber threats," *Future Gener. Comput. Syst.*, vol. 83, pp. 535–552, Jun. 2018, doi: [10.1016/j.future.2017.05.043](https://doi.org/10.1016/j.future.2017.05.043).
- [140] N. Herold, "Incident handling systems with automated intrusion response," Ph.D. dissertation, Dept. Inf., Tech. Univ. Munich, Munich, Germany, 2017.
- [141] K. Hughes, K. McLaughlin, and S. Sezer, "Dynamic countermeasure knowledge for intrusion response systems," in *Proc. 31st Irish Signals Syst. Conf. (ISSC)*, Letterkenny, Ireland, Jun. 2020, pp. 1–6.
- [142] S. Iannucci and S. Abdelwahed, "Towards autonomous intrusion response systems," in *Proc. IEEE Int. Conf. Autonomous Comput. (ICAC)*, Wuerzburg, Germany, Jul. 2016, pp. 229–230.
- [143] S. Iannucci and S. Abdelwahed, "Model-based response planning strategies for autonomous intrusion protection," *ACM Trans. Auto. Adapt. Syst.*, vol. 13, no. 1, pp. 1–23, Mar. 2018, doi: [10.1145/3168446](https://doi.org/10.1145/3168446).
- [144] S. Iannucci, V. Cardellini, O. D. Barba, and I. Banicescu, "A hybrid model-free approach for the near-optimal intrusion response control of non-stationary systems," *Future Gener. Comput. Syst.*, vol. 109, pp. 111–124, Aug. 2020, doi: [10.1016/j.future.2020.03.018](https://doi.org/10.1016/j.future.2020.03.018).
- [145] S. Iannucci, Q. Chen, and S. Abdelwahed, "High-performance intrusion response planning on many-core architectures," in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Waikoloa, HI, USA, Aug. 2016, pp. 1–6. [Online]. Available: <https://www.cci.msstate.edu/publications/docs/2016/08/14406nsaa16.pdf>
- [146] D. Jadhav, N. Patil, P. Deshmukh, R. Patil, and R. Dixit, "RRE: Network intrusion detection and game-theoretic for response strategy for automated," *Int. J. Eng. Tech. Res.*, vol. 3, no. 10, pp. 1–10, Oct. 2015.
- [147] M. Jahnke, J. Tölle, C. Thul, and P. Martini, "Validating GrADAR—An approach for graph-based automated DoS attack response," in *Proc. IEEE 34th Conf. Local Comput. Netw.*, Zurich, Switzerland, Oct. 2009, pp. 225–228.
- [148] N. B. A. Jumaat, "Incident prioritisation for intrusion response systems," Ph.D. dissertation, Dept. Sci. Technol., Univ. Plymouth, Plymouth, U.K., 2012.
- [149] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, and J. Araujo, "Automated reaction based on risk analysis and attackers skills in intrusion detection systems," in *Proc. 3rd Int. Conf. Risks Secur. Internet Syst.*, Oct. 2008, pp. 117–124.
- [150] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, and F. Autrel, "Advanced reaction using risk assessment in intrusion detection systems," in *Proc. Int. Workshop Crit. Inf. Infrastructures Secur.*, Málaga, Spain, Oct. 2008, pp. 58–70.
- [151] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, S. Dubus, and A. Martin, "Success likelihood of ongoing attacks for intrusion detection and response systems," in *Proc. Int. Conf. Comput. Sci. Eng.*, vol. 3, Vancouver, BC, Canada, Aug. 2009, pp. 83–91.
- [152] N. Kheir, H. Debar, F. Cuppens, N. Cuppens-Boulahia, and J. Viinikka, "A service dependency modeling framework for policy-based response enforcement," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*, Milan, Italy, Jul. 2009, pp. 176–195.
- [153] J. Kim, K. Kim, and J. Jang, "Policy-based intrusion detection and automated response mechanism," in *Proc. Int. Conf. Inf. Netw.*, 2002, pp. 399–408.
- [154] B. Lang, J. Liu, and J. Zheng, "The research on automated intrusion response system based on mobile agents," in *Proc. 8th Int. Conf. Comput. Supported Cooperat. Work Design*, Xiamen, China, May 2004, pp. 344–347.
- [155] S. M. Lewandowski, D. J. van Hook, G. C. O'Leary, J. W. Haines, and L. M. Rossey, "SARA: Survivable autonomous response architecture," in *Proc. DARPA Inf. Survivability Conf. Expo.*, Anaheim, CA, USA, Jan. 2001, pp. 77–88.
- [156] F. Li, Y. Li, S. Leng, Y. Guo, K. Geng, Z. Wang, and L. Fang, "Dynamic countermeasures selection for multi-path attacks," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101927, doi: [10.1016/j.cose.2020.101927](https://doi.org/10.1016/j.cose.2020.101927).
- [157] X. Li, C. Zhou, Y.-C. Tian, and Y. Qin, "A dynamic decision-making approach for intrusion response in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2544–2554, May 2019, doi: [10.1109/TII.2018.2866445](https://doi.org/10.1109/TII.2018.2866445).
- [158] S. Liu, T. Li, K. Zhao, J. Yang, X. Gong, and J. Zhang, "Immune-based dynamic intrusion response model," in *Proc. Asia-Pacific 6th Int. Conf. Simulated Evol. Learn.*, Oct. 2006, pp. 96–103.
- [159] Z. Liu and R. Uppala, "A dynamic countermeasure method for large-scale network attacks," in *Proc. 2nd IEEE Int. Symp. Dependable, Autonomous Secure Comput.*, Sep. 2006, pp. 163–170.
- [160] C. Mu, X. Li, H. Huang, and S. Tian, "Online risk assessment of intrusion scenarios using DS evidence theory," in *Proc. Eur. Symp. Res. Comput. Secur.*, Málaga, Spain, 2008, pp. 35–48.
- [161] C.-P. Mu, H.-K. Huang, and S.-F. Tian, "Fuzzy cognitive maps for decision support in an automatic intrusion response mechanism," in *Proc. Int. Conf. Mach. Learn. Cybern.*, Shanghai, China, Aug. 2004, pp. 1789–1794.
- [162] A. Nadeem, "Intrusion detection & prevention mechanism for mobile ad hoc networks," Ph.D. dissertation, Dept. Electron. Phys. Sci, Univ. Surrey, Guildford, U.K., 2010.
- [163] L.-X. Peng and T.-W. Chen, "Automated intrusion response system algorithm with danger theory," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Shanghai, China, Oct. 2014, pp. 31–34.
- [164] Y. Ping, Z. Futai, J. Xinghao, and L. Jianhua, "Multi-agent cooperative intrusion response in mobile adhoc networks," *J. Syst. Eng. Electron.*, vol. 18, no. 4, pp. 785–794, Dec. 2007, doi: [10.1016/S1004-4132\(08\)60021-3](https://doi.org/10.1016/S1004-4132(08)60021-3).
- [165] N. Poolsappisit, R. Dewri, and I. Ray, "Dynamic security risk management using Bayesian attack graphs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 61–74, Jan. 2012, doi: [10.1109/TDSC.2011.34](https://doi.org/10.1109/TDSC.2011.34).

- [166] A. M. Resmi and R. M. Chezian, "An extension of intrusion prevention, detection and response system for secure content delivery networks," in *Proc. IEEE Int. Conf. Adv. Comput. Appl. (ICACA)*, Coimbatore, India, Oct. 2016, pp. 144–149.
- [167] J. R. Rose, M. Swann, K. P. Grammatikakis, I. Koufos, G. Bendiab, S. Shialeles, and N. Kolokotronis, "IDERES: Intrusion detection and response system using machine learning and attack graphs," *J. Syst. Archit.*, vol. 131, Oct. 2022, Art. no. 102722, doi: 10.1016/j.sysarc.2022.102722.
- [168] J. Rowanhill, G. Wasson, Z. Hill, J. Basney, Y. Kiryakov, J. Knight, A. Nguyen-Tuong, A. Grimshaw, and M. Humphrey, "Dynamic system-wide reconfiguration of grid deployments in response to intrusion detections," in *Proc. Int. Conf. High Perform. Comput. Commun.*, 2007, pp. 260–272.
- [169] T. Rytov, C. Neuman, and D. Kim, "Dynamic authorization and intrusion response in distributed systems," in *Proc. DARPA Inf. Survivability Conf. Expo.*, Washington, DC, USA, Apr. 2003, pp. 50–61.
- [170] J. K. Samarabandu, "Keynote address: Dynamic network security-intrusion detection and response," in *Proc. Moratuwa Eng. Res. Conf. (MERCOn)*, Moratuwa, Sri Lanka, Apr. 2016, pp. 105–116.
- [171] D. Schnackengerg, H. Holliday, R. Smith, K. Djahandari, and D. Sterne, "Cooperative intrusion traceback and response architecture (CITRA)," in *Proc. DARPA Inf. Survivability Conf. Expo.*, Anaheim, CA, USA, Jan. 2001, pp. 56–68.
- [172] M. Shajari and A. A. Ghorbani, "Application of belief-desire-intention agents in intrusion detection & response," in *Proc. Ann. Conf. Privacy Secur. Trust (PST)*, 2004, pp. 181–191. [Online]. Available: <https://www.researchgate.net/publication/220919897>
- [173] A. Shameli-Sendi, H. Louafi, W. He, and M. Cheriet, "Dynamic optimal countermeasure selection for intrusion response system," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 755–770, Sep. 2018, doi: 10.1109/TDSC.2016.2615622.
- [174] R. K. Sharma, B. Issac, and H. K. Kalita, "Intrusion detection and response system inspired by the defense mechanism of plants," *IEEE Access*, vol. 7, pp. 52427–52439, 2019, doi: 10.1109/ACCESS.2019.2912114.
- [175] K. K. Singh, "A trust-based model for collaborative intrusion response," M.S. thesis, Dept. Comput. Sci., Univ. Brit. Columbia, Vancouver, BC, Canada, 2005.
- [176] C. Strasburg, S. Basu, and J. S. Wong, "S-MAIDS: A semantic model for automated tuning, correlation, and response selection in intrusion detection systems," in *Proc. IEEE 37th Annu. Comput. Softw. Appl. Conf.*, Kyoto, Japan, Jul. 2013, pp. 319–328.
- [177] S. Sultana, D. Midi, and E. Bertino, "Kinesis: A security incident response and prevention system for wireless sensor networks," in *Proc. 12th ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2014, pp. 148–162.
- [178] S. Ullah, S. Shelly, A. Hassanzadeh, A. Nayak, and K. Hasan, "On the effectiveness of intrusion response systems against persistent threats," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Big Island, HI, USA, Feb. 2020, pp. 415–421.
- [179] X. Wang, D. S. Reeves, and S. F. Wu, "Tracing based active intrusion response," *J. Inf. Warfare*, vol. 1, no. 1, pp. 50–61, 2001.
- [180] X. Wang, D. S. Reeves, S. F. Wu, and J. Yuill, "Sleepy watermark tracing: An active network-based intrusion response framework," in *Proc. IFIP Int. Inf. Secur. Conf.*, Boston, MA, USA, 2001, pp. 369–384.
- [181] Z. Wang, Q. Zhao, H. Wang, and L. Yu, "MAIRF: An approach to mobile agents-based intrusion response system," in *Proc. 1ST IEEE Conf. Ind. Electron. Appl.*, Singapore, May 2006, pp. 1–4.
- [182] Z.-Q. Wang, H.-Q. Wang, and R.-J. Zhang, "Analysis of an intelligent agent intrusion response system," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Intell. Agent Technol. Workshops*, Hong Kong, Dec. 2006, pp. 53–56.
- [183] X. Zan, F. Gao, J. Han, X. Liu, and J. Zhou, "NAIR: A novel automated intrusion response system based on decision making approach," in *Proc. IEEE Int. Conf. Inf. Autom.*, Harbin, China, Jun. 2010, pp. 543–548.
- [184] W. Zeng-quan, W. Hui-qiang, and Z. Rui-jie, "Research and design on intelligent agent intrusion response system," in *Proc. Int. Conf. Comput. Intelligence Model. Control Autom. Int. Conf. Intell. Agents Web Technol. Int. Commerce (CIMCA)*, Nov. 2006, p. 231.
- [185] S. A. Zonouz, "Game-theoretic intrusion response and recovery," Ph.D. dissertation, Dept. Comput. Sci., Univ. Illinois, Urbana, IL, USA, 2011.
- [186] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A game-theoretic intrusion response and recovery engine," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 395–406, Feb. 2014, doi: 10.1109/TPDS.2013.211.
- [187] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in *Proc. DARPA Inf. Survivability Conf. Expo.*, Washington, DC, USA, Apr. 2003, pp. 303–314.
- [188] D. Hosiadi and I. M. Susila, "Improving automatic response model system for intrusion detection system," in *Proc. The 1st Int. Conf. Comput. Sci. Eng. Technol. Universitas Muria Kudus*, Kudus, Indonesia, Oct. 2018, pp. 449–457.
- [189] A. Mitrokotsa, N. Komninos, and C. Douligeris, "Intrusion detection and response in ad hoc networks," *Int. J. Comput. Res.*, vol. 15, no. 1, pp. 23–55, 2007.
- [190] A. Mitrokotsa, N. Komninos, and C. Douligeris, "Towards an effective intrusion response engine combined with intrusion detection in ad hoc networks," 2008, *arXiv:0807.2053*.
- [191] S. Mnsman and P. Flesher, "System or security managers adaptive response tool," in *Proc. DARPA Inf. Survivability Conf. Expo.*, Hilton Head, SC, USA, Jan. 2000, pp. 56–68.
- [192] R. Parti, "Design of an intrusion response system using evolutionary computation," Dept. Comput. Sci., Univ. Missouri, Columbia, MO, USA, Tech. Rep. CS401, Dec. 2003, pp. 1–40.
- [193] F. Patzer, P. Lütke, A. Meshram, and J. Beyerer, "Context-aware software-defined networking for automated incident response in industrial networks," in *Proc. 5th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, 2020, pp. 137–161.
- [194] F. Patzer, A. Meshram, and M. Heß, "Automated incident response for industrial control systems leveraging software-defined networking," in *Proc. 5th Int. Conf. Inf. Syst. Secur. Privacy*, 2019, pp. 319–327.
- [195] A. Somayaji and S. Forrest, "Automated response using system-call delay," in *Proc. 9th USENIX Secur. Symp.*, Denver, CO, USA, Aug. 2000, pp. 185–197.
- [196] P. Yi, Y. Zhong, and S. Zhang, "Applying mobile agent to intrusion response for ad hoc networks," in *Proc. Int. Conf. Comput. Sci. Eng.*, Atlanta, GA, USA, May 2005, pp. 593–600.
- [197] J. Barrus and N. C. Rowe, "A distributed autonomous-agent network-intrusion detection and response system," Nav. Postgraduate School, Monterey, CA, USA, Tech. Rep. 0704-0188, 1988.
- [198] Z. Cai, Q. Zhang, and Y. Gan, "Intrusion intention recognition and response based on weighed plan knowledge graph," *Comput. Model. New Technol.*, vol. 18, no. 12, pp. 151–157, 2014.
- [199] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proc. 6th ACM Symp. Inf., Comput. Commun. Secur.*, Hong Kong, Mar. 2011, pp. 355–366. [Online]. Available: [https://feihu.eng.ua.edu/NSF\\_CPS/year1/w8\\_3.pdf](https://feihu.eng.ua.edu/NSF_CPS/year1/w8_3.pdf)
- [200] F. Cuppens, F. Autrel, Y. Bouzida, J. Garcia, S. Gombault, and T. Sans, "Anti-correlation as a criterion to select appropriate counter-measures in an intrusion detection framework," *Ann. Des. Telecommun.*, vol. 61, nos. 1–2, pp. 197–217, Feb. 2006, doi: 10.1007/bf03219974.
- [201] F. Cuppens, S. Gombault, and T. Sans, "Selecting appropriate counter-measures in an intrusion detection framework," in *Proc. 17th IEEE Comput. Secur. Found. Workshop*, Pacific Grove, CA, USA, Jun. 2004, pp. 78–87.
- [202] E. Doynikova and I. Kotenko, "The multi-layer graph based technique for proactive automatic response against cyber attacks," in *Proc. 26th Euromicro Int. Conf. Parallel, Distrib. Network-based Process. (PDP)*, Mar. 2018, pp. 470–477.
- [203] M. Gangadharan and K. Hwang, "Intranet security with micro-firewalls and mobile agents for proactive intrusion response," in *Proc. Int. Conf. Comput. Netw. Mobile Comput.*, Beijing, China, Oct. 2001, pp. 325–332.
- [204] M. Hamad, M. Tsantekidis, and V. Prevelakis, "Red-zone: Towards an intrusion response framework for intra-vehicle system," in *Proc. 5th Int. Conf. Vehicle Technol. Intell. Transp. Syst.*, 2019, pp. 148–158.
- [205] S. Jajodia and S. Noel, "Topological vulnerability analysis: A powerful new approach for network attack prevention, detection, and response," in *Algorithms, Architectures and Information Systems Security*, vol. 3, B. B. Bhattacharya, S. S. Kolay, S. C. Nandy, and A. Bagchi, Eds. Singapore: World Scientific, 2008, ch. 13, pp. 285–305.



- [206] W. Jiang, Z.-H. Tian, H.-L. Zhang, and X.-F. Song, "A stochastic game theoretic approach to attack prediction and optimal active defense strategy decision," in *Proc. IEEE Int. Conf. Netw., Sens. Control*, Sanya, China, Apr. 2008, pp. 648–653.
- [207] S. Noel and S. Sajodia, "Proactive intrusion prevention and response via attack graphs," in *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century: Prevention and Detection for the Twenty-First Century*, 1st ed. Reading, MA, USA: Addison-Wesley, 2009, ch. 5.
- [208] L. S. Ramachandra and K. Hareesh, "A novel design for real-time intrusion response in latest software-defined networks by graphical security models," in *Sustainable Communication Networks and Application*. Singapore: Springer, 2021, pp. 557–568.
- [209] S. Shen, K. Hu, L. Huang, H. Li, R. Han, and Q. Cao, "Quantal response equilibrium-based strategies for intrusion detection in WSNs," *Mobile Inf. Syst.*, vol. 2015, pp. 1–10, Aug. 2015, doi: [10.1155/2015/179839](https://doi.org/10.1155/2015/179839).
- [210] I. Svecs, T. Sarkar, S. Basu, and J. S. Wong, "XIDR: A dynamic framework utilizing cross-layer intrusion detection for effective response deployment," in *Proc. IEEE 34th Annu. Comput. Softw. Appl. Conf. Workshops*, Jul. 2010, pp. 287–292.
- [211] M. G. Uddin, H. Shahriar, and M. Zulkernine, "ACIR: An aspect-connector for intrusion response," in *Proc. 31st Annu. Int. Comput. Softw. Appl. Conf.*, vol. 2, Beijing, China, Jul. 2007, pp. 249–254.
- [212] C. Zhang, X. Costa-Pérez, and P. Patras, "Adversarial attacks against deep learning-based network intrusion detection systems and defense mechanisms," *IEEE/ACM Trans. Netw.*, vol. 30, no. 3, pp. 1294–1311, Jun. 2022, doi: [10.1109/TNET.2021.3137084](https://doi.org/10.1109/TNET.2021.3137084).
- [213] F. Zhang, Z. Qin, and S. Zhou, "Policy-tree based proactive defense model for network security," in *Proc. Int. Conf. Grid Cooperat. Comput.*, Oct. 2004, pp. 437–449.
- [214] Z. Zhang, F. Naït-Abdesselam, P.-H. Ho, and Y. Kadobayashi, "Toward cost-sensitive self-optimizing anomaly detection and response in automatic networks," *Comput. Secur.*, vol. 30, nos. 6–7, pp. 525–537, Sep. 2011, doi: [10.1016/j.cose.2011.06.002](https://doi.org/10.1016/j.cose.2011.06.002).
- [215] T. Hussain, C. Nugent, J. Liu, A. Beard, L. Chen, and A. Moore, "An attack impact and host importance based approach to intrusion response action selection," in *Proc. 4th Int. Conf. Inf. Technol. Comput. Commun. (ITCC)*, Jun. 2022, pp. 84–91, doi: [10.1145/3548636.3548649](https://doi.org/10.1145/3548636.3548649).
- [216] Y. Laaboudi, A. Olivereau, and N. Oualha, "An intrusion detection and response scheme for CP-ABE-encrypted IoT networks," in *Proc. 10th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Canary Islands, Spain, Jun. 2019, pp. 1–5.
- [217] N. Foukia, S. Hassas, and S. Fenet, "An intrusion response scheme: Tracking the alert source using a stigmergy paradigm," in *Proc. 2nd Int. Workshop Secur. Mobile Multiagent Syst.*, Aug. 2002, pp. 1–9. [Online]. Available: <https://www.researchgate.net/publication/228792931>
- [218] P. García-Teodoro, J. E. Díaz-Verdejo, G. Maciá-Fernández, and L. Sánchez-Casad, "Network-based hybrid intrusion detection and honeypots as active reaction schemes," *Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 10, p. 62, Oct. 2007.
- [219] J. S. Goodgion, "Active response using host-based intrusion detection system and software-defined networking," M.S. thesis, Dept. Elect. Comput. Eng., Air Univ., Montgomery, AL, USA, 2017.
- [220] H. Han, X.-L. Lu, L.-Y. Ren, and B. Chen, "Taichi: An open intrusion automatic response system based on plugin," in *Proc. Int. Conf. Mach. Learn. Cybern.*, Dalian, China, Aug. 2006, pp. 66–77.
- [221] A. Hess, M. Jung, and G. Schäfer, "Combining multiple intrusion detection and response technologies in an active networking based architecture," in *Proc. Secur., E-Learn., E-Services, DFN-Arbeitsstagung Über Kommunikationsnetze*, 2003, pp. 153–164.
- [222] H.-P. Huang and C.-M. Chang, "An active network-based intrusion detection and response systems," in *Proc. IEEE Int. Conf. Netw., Sens. Control*, Taipei, Taiwan, Mar. 2004, pp. 1317–1322.
- [223] Y. Jiang and J. Chang, "Intrusion prevention system base on immune vaccination," in *Proc. 2nd Int. Conf. Intell. Comput. Technol. Autom.*, Changsha, China, Oct. 2009, pp. 350–353.
- [224] Y.-X. Lim, T. S. Yer, J. Levine, and H. L. Owen, "Wireless intrusion detection and response," in *Proc. IEEE Syst., Man Cybern. Soc. Inf. Assurance Workshop*, West Point, NY, USA, Jun. 2003, pp. 68–75.
- [225] S. Salekzamankhani, A. Pakstas, and B. Virdee, "Ontology approach to construction of response and management console subsystems for intrusion handling systems in wireless LANs," in *Proc. World Congr. Eng.*, London, U.K., 2010, pp. 1–6. [Online]. Available: <https://www.researchgate.net/publication/45534494>
- [226] S. T. Sawant and B. S. Nitin, "Network intrusion detection and response system for mobile ad hoc networks," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 2, no. 5, pp. 75–80, 2013.
- [227] J. L. Thames, R. Abler, and D. Keeling, "A distributed firewall and active response architecture providing preemptive protection," in *Proc. 46th Annu. Southeast Regional Conf.*, Mar. 2008, pp. 220–225.
- [228] J. Lane Thames, R. Abler, and D. Keeling, "A distributed active response architecture for preventing SSH dictionary attacks," in *Proc. IEEE SoutheastCon*, Huntsville, AL, USA, Apr. 2008, pp. 84–89.
- [229] X. Ye, J. Li, and R. Luo, "Hide Markov model based intrusion detection and response for manets," in *Proc. 2nd Int. Conf. Inf. Technol. Comput. Sci.*, Kiev, Ukraine, Jul. 2010, pp. 142–145.
- [230] S. Yoon, J.-H. Cho, G. Dixit, and I.-R. Chen, "Resource-aware intrusion response based on deep reinforcement learning for software-defined Internet-of-Battle-Things," in *Game Theory and Machine Learning for Cyber Security*, C. A. Kamhoua, C. D. Kiekintveld, F. Fang, and Q. Zhu, Eds. Hoboken, NJ, USA: Wiley, 2021, ch. 20.
- [231] M. Zaki and T. S. Sobh, "Design of an active security multi-agent intrusion detection system," *Asian J. Inf. Technol.*, vol. 3, no. 1, pp. 1–10, Oct. 2004.
- [232] C. W. Meng, "Applying mobile agents technology to intrusion detection and response," M.S. thesis, Dept. Comput. Sci., Nat. Univ. Singap., Queenstown, New Zealand, 2004.
- [233] V. Cardellini, E. Casalicchio, S. Iannucci, M. Lucantonio, S. Mittal, D. Panigrahi, and A. Silvi, "An intrusion response system utilizing deep Q-networks and system partitions," *SoftwareX*, vol. 19, Jul. 2022, Art. no. 101120, doi: [10.1016/j.softx.2022.101120](https://doi.org/10.1016/j.softx.2022.101120).
- [234] C. Carver, J. Hill, J. R. Surdu, and U. W. Pooch, "A methodology for using intelligent agents to provide automated intrusion response," in *Proc. IEEE Syst., Man, Cybern. Inf. Assurance Secur. Workshop*, West Point, NY, USA, Jun. 2000, pp. 110–116. [Online]. Available: [https://www.west-point.org/users/usma1982/39377/john/Publications/2000/2000-06\\_SMC-IAW/AutoIR/](https://www.west-point.org/users/usma1982/39377/john/Publications/2000/2000-06_SMC-IAW/AutoIR/)
- [235] C. A. Carver, J. M. Hill, and U. W. Pooch, "Limiting uncertainty in intrusion response," in *Proc. IEEE Workshop Inf. Assurance Secur.*, West Point, NY, USA, Jan. 2001, pp. 5–6.
- [236] C. A. Carver, "Adaptive agent-based intrusion response," Ph.D. dissertation, Dept. Comput. Sci., Texas A&M Univ., College Station, TX, USA, 2001.
- [237] B. Foo, Y.-S. Wu, Y.-C. Mao, S. Bagchi, and E. Spafford, "ADEPTS: Adaptive intrusion response using attack graphs in an e-commerce environment," in *Proc. Int. Conf. Dependable Syst. Netw. (DSN)*, Yokohama, Japan, Jun. 2005, pp. 508–517.
- [238] C. H. Gan, A. Zaslavsky, and S. Giles, "CAWAnalysr: Enhancing wireless intrusion response with runtime context-awareness," in *Proc. Int. Conf. Netw.*, Apr. 2005, pp. 239–246.
- [239] R. S. Hajari and V. G. Kasabegoudar, "Risk aware intrusion detection and response mechanism for MANET," *Int. J. Comput. Appl.*, vol. 112, no. 15, pp. 30–33, Feb. 2015.
- [240] K. Hammar and R. Stadler, "Learning near-optimal intrusion responses against dynamic attackers," 2023, *arXiv:2301.06085*.
- [241] A. Hess, M. Jung, and G. Schafer, "FIDRAN: A flexible intrusion detection and response framework for active networks," in *Proc. 8th IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2003, pp. 1219–1224.
- [242] P. Holgado and V. A. Villagra, "Neural networks applied to the learning process of automated intrusion response systems," presented at the Actas Primeras Jornadas Nacionales Investigación Ciberseguridad (JNIC), Sep. 2015.
- [243] K. Hughes, K. McLaughlin, and S. Sezer, "A model-free approach to intrusion response systems," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103150, doi: [10.1016/j.jisa.2022.103150](https://doi.org/10.1016/j.jisa.2022.103150).
- [244] K. Karunanidhi, "ARROS: Distributed adaptive real-time network intrusion response," M.S. thesis, Dept. Russ College Eng. Technol., Ohio Univ., Athens, OH, USA, 2006.
- [245] G. Klein, H. Rogge, F. Schneider, J. Toelle, M. Jahnke, and S. Karsch, "Response initiation in distributed intrusion response systems for tactical MANETs," in *Proc. Eur. Conf. Comput. Netw. Defense*, Berlin, Germany, Oct. 2010, pp. 55–62.
- [246] V. M. Lanchas, V. A. V. González, and F. R. Bueno, "Ontologies-based automated intrusion response system," in *Computational Intelligence in Security for Information Systems*. Berlin, Germany: Springer, 2010, pp. 99–106.

- [247] F. Li, F. Xiong, C. Li, L. Yin, G. Shi, and B. Tian, "SRAM: A state-aware risk assessment model for intrusion response," in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace (DSC)*, Shenzhen, China, Jun. 2017, pp. 232–237.
- [248] Y. Luo, F. Szidarovszky, Y. Al-Nashif, and S. Hariri, "A fictitious play-based response strategy for multistage intrusion defense systems," *Secur. Commun. Netw.*, vol. 7, no. 3, pp. 473–491, Mar. 2014, doi: 10.1002/sec.730.
- [249] K. Malialis, "Distributed reinforcement learning for network intrusion response," Ph.D. dissertation, Dept. Comput. Sci., York Univ., Heslington, U.K., 2014.
- [250] K. Malialis, S. Devlin, and D. Kudenko, "Distributed reinforcement learning for adaptive and robust network intrusion response," *Connection Sci.*, vol. 27, no. 3, pp. 234–252, Apr. 2015, doi: 10.1080/09540091.2015.1031082.
- [251] V. Mateos, V. A. Villagrà, F. Romero, and J. Berrocal, "Definition of response metrics for an ontology-based automated intrusion response systems," *Comput. Electr. Eng.*, vol. 38, no. 5, pp. 1102–1114, Sep. 2012, doi: 10.1016/j.compeleceng.2012.06.001.
- [252] A. Nadeem and M. P. Howarth, "An intrusion detection & adaptive response mechanism for MANETs," *Ad Hoc Netw.*, vol. 13, pp. 368–380, Feb. 2014, doi: 10.1016/j.adhoc.2013.08.017.
- [253] J. Nyberg, P. Johnson, and A. Méhes, "Cyber threat response using reinforcement learning in graph-based attack simulations," in *Proc. IEEE/IFIP Netw. Operations Manage. Symp.*, Budapest, Hungary, Apr. 2022, pp. 1–4.
- [254] M. Petkac and L. Badger, "Security agility in response to intrusion detection," in *Proc. 16th Annu. Comput. Secur. Appl. Conf.*, New Orleans, LA, USA, Dec. 2000, pp. 11–20.
- [255] T. V. Phan and T. Bauschert, "DeepAir: Deep reinforcement learning for adaptive intrusion response in software-defined networks," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 3, pp. 2207–2218, Sep. 2022, doi: 10.1109/TNSM.2022.3158468.
- [256] S. N. Pujar, G. Choudhary, S. K. Shandilya, V. Sihag, and A. Choudhary, "An adaptive auto incident response based security framework for wireless network systems," *Res. Briefs Inf. Commun. Technol. Evol.*, vol. 7, p. 4, Aug. 2021, doi: 10.22667/ReBiCTE.2021.08.15.004.
- [257] S. Ramesh, S. Selvarayan, K. Sunil, and C. Arumugam, "An adaptive multi-layered approach for DoS detection and mitigation," in *Proc. Int. Conf. Comput. Sci. Appl.*, Sep. 2021, pp. 533–545.
- [258] A. Shameli-Sendi, J. Desfossez, M. Dagenais, and M. Jabbarifar, "A retroactive-burst framework for automated intrusion response system," *J. Comput. Netw. Commun.*, vol. 2013, pp. 1–8, Apr. 2013, doi: 10.1155/2013/134760.
- [259] R. K. Sharma, H. K. Kalita, and B. Issac, "PIRIDS: A model on intrusion response system based on biologically inspired response mechanism in plants," in *Proc. Int. Conf. Innov. Bio-Inspired Comput. Appl. (IBICA)*, Dec. 2016, pp. 105–116.
- [260] Z. S. Stefanova and K. M. Ramachandran, "Off-policy Q-learning technique for intrusion response in network security," *Int. J. Comput. Inf. Eng.*, vol. 12, no. 4, pp. 262–268, 2018.
- [261] B. Wang, Y. Sun, M. Sun, and X. Xu, "Game-theoretic actor-critic-based intrusion response scheme (GTAC-IRS) for wireless SDN-based IoT networks," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1830–1845, Feb. 2021, doi: 10.1109/JIOT.2020.3015042.
- [262] Y.-S. Wu, B. Foo, Y.-C. Mao, S. Bagchi, and E. H. Spafford, "Automated adaptive intrusion containment in systems of interacting services," *Comput. Netw.*, vol. 51, no. 5, pp. 1334–1360, Apr. 2007, doi: 10.1016/j.comnet.2006.09.006.
- [263] Y.-S. Wu, B. Foo, B. Matheny, T. Olsen, and S. Bagchi, "ADEPTS: Adaptive intrusion containment and response using attack graphs in an e-commerce environment," School Elect. Comput. Eng., Purdue Univ., West Lafayette, IN, India, Tech. Rep. 32, 2003.
- [264] Y.-S. Wu, G. Howard, M. Glause, B. Foo, S. Bagchi, and E. Spafford, "The search for optimality in online intrusion response for a distributed e-commerce system," Dept. Inf. Assurance Secur. Educ. Center, Purdue Univ., West Lafayette, IN, India, Tech. Rep. 94, 2007.
- [265] Y.-S. Wu, G. Modelo-Howard, B. Foo, S. Bagchi, and E. H. Spafford, "The search for efficiency in automated intrusion response for distributed applications," in *Proc. Symp. Reliable Distrib. Syst.*, Naples, Italy, Oct. 2008, pp. 53–62.
- [266] Z. Wu, D. Xiao, H. Xu, X. Peng, and X. Zhuang, "Automated intrusion response decision based on the analytic hierarchy process," in *Proc. IEEE Int. Symp. Knowl. Acquisition Model. Workshop*, Wuhan, China, Dec. 2008, pp. 574–577.
- [267] J.-N. Yang, H.-Q. Zhang, and C.-F. Zhang, "Intrusion response decision-making method based on reinforcement learning," in *Proc. Int. Conf. Commun. Netw. Artif. Intell. (CNAI)*, Jul. 2018, pp. 1–9. [Online]. Available: <http://www.dpi-proceedings.com/index.php/dtcese/article/download/24149/23783>
- [268] Z. Asgharian, H. Asgharian, A. Akbari, and B. Raahemi, "A framework for SIP intrusion detection and response systems," in *Proc. Int. Symp. Comput. Netw. Distrib. Syst. (CNDS)*, Tehran, Iran, Feb. 2011, pp. 100–105.
- [269] M. A. Azer, S. M. El-Kassas, and M. S. El-Soudani, "A scheme for intrusion detection and response in ad hoc networks," in *New Technologies, Mobility and Security*, vol. 42, 1st ed., H. Labiod and M. Badra, Eds. Dordrecht, The Netherlands: Springer, 2007, pp. 507–516.
- [270] A. O. Bang, U. P. Rao, P. Kaliyar, and M. Conti, "Assessment of routing attacks and mitigation techniques with RPL control messages: A survey," *ACM Comput. Surv.*, vol. 55, no. 2, pp. 1–36, Jan. 2022, doi: 10.1145/3494524.
- [271] N. Foukia, "IDReAM: Intrusion detection and response executed with agent mobility architecture and implementation," in *Proc. 4th Int. Joint Conf. Auto. Agents Multiagent Syst.*, Jul. 2005, pp. 264–270.
- [272] W. Gao, T. Morris, B. Reeves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. eCrime Researchers Summit*, Oct. 2010, pp. 1–9.
- [273] S. Ji, C. Im, M. Kim, and H. Jeong, "Botnet detection and response architecture for offering secure Internet services," in *Proc. Int. Conf. Secur. Technol.*, Sanya, China, Dec. 2008, pp. 101–104.
- [274] D. Kashiwa, E. Y. Chen, and H. Fuji, "Active shaping: A countermeasure against DDoS attacks," in *Proc. 2nd Eur. Conf. Universal Multiservice Netw.*, Colmar, France, Apr. 2002, pp. 171–179.
- [275] M. Khabbazi, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 736–745, Feb. 2009, doi: 10.1109/TWC.2009.070536.
- [276] C. Lee, S. M. Han, Y. H. Chae, and P. H. Seong, "Development of a cyberattack response planning method for nuclear power plants by using the Markov decision process model," *Ann. Nucl. Energy*, vol. 166, Feb. 2022, Art. no. 108725, doi: 10.1016/j.anucene.2021.108725.
- [277] D. H. Lee, J. M. Kim, K.-H. Choi, and K. J. Kim, "The study of response model & mechanism against windows kernel compromises," in *Proc. Int. Conf. Conver. Hybrid Inf. Technol.*, Aug. 2008, pp. 600–608.
- [278] F. Medjek, D. Tandjaoui, N. Djedjig, and I. Romdhani, "Multicast DIS attack mitigation in RPL-based IoT-LLNs," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102939, doi: 10.1016/j.jisa.2021.102939.
- [279] R. Mohammadi, R. Javidan, and M. Conti, "SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks," *IEEE Trans. Netw. Service Manage.*, vol. 14, no. 2, pp. 487–497, Jun. 2017, doi: 10.1109/TNSM.2017.2701549.
- [280] S. M. Moosavirad, P. Kabiri, and H. Mahini, "Rashnu: A Wi-Fi intrusion response scheme," *Secur. Commun. Netw.*, vol. 8, no. 12, pp. 2070–2078, Aug. 2015, doi: 10.1002/sec.1153.
- [281] V. Pruthi, K. Mittal, N. Sharma, and I. Kaushik, "Network layers threats & its countermeasures in WSNs," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Greater Noida, India, Oct. 2019, pp. 156–163.
- [282] G. Rajendran, R. S. R. Nivash, P. P. Parthy, and S. Balamurugan, "Modern security threats in the Internet of Things (IoT): Attacks and countermeasures," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Chennai, India, Oct. 2019, pp. 1–6.
- [283] M. Reháč, M. Pichouček, D. Medvigy, M. Prokopová, J. Tožička, and L. Foltýn, "Agent methods for network intrusion detection and response," in *Proc. Int. Conf. Ind. Appl. Holonic Multi-Agent Syst.*, Sep. 2007, pp. 149–160.
- [284] T. R. Schmoeyer, Y. Xi Lim, and H. L. Owen, "Wireless intrusion detection and response: A classic study using main-in-the-middle attack," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Atlanta, GA, USA, 2004, pp. 883–888.
- [285] M. Surendar and A. Umamakeswari, "InDReS: An intrusion detection and response system for Internet of Things with 6LoWPAN," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WISPNET)*, Chennai, India, Mar. 2016, pp. 1903–1908.

- [286] B. Todtmann, S. Riebach, and E. P. Rathgeb, "The honeynet quarantine: Reducing collateral damage caused by early intrusion response," in *Proc. 6th Int. Conf. Netw. (ICN)*, Apr. 2007, p. 96.
- [287] Z. Wu, D. Xiao, H. Xu, X. Peng, and X. Zhuang, "Virtual inline: A technique of combining IDS and IPS together in response intrusion," in *Proc. 1st Int. Workshop Educ. Technol. Comput. Sci.*, Wuhan, China, Mar. 2009, pp. 1118–1121.
- [288] P. J. Yurkovich, "RSU-based intrusion detection and autonomous intersection response systems," M.S. thesis, Dept. Civil Eng., Virginia Polytech. Univ., Blacksburg, VA, USA, 2022.
- [289] S. T. Zargar and J. B. D. Joshi, "A collaborative approach to facilitate intrusion detection and response against DDoS attacks," in *Proc. 6th Int. Conf. Collaborative Computing: Netw., Appl. Worksharing (CollaborateCom)*, Chicago, IL, USA, Oct. 2010, pp. 1–8. [Online]. Available: <https://eudl.eu/pdf/10.4108/icst.collaboratecom.2010.46>
- [290] (2012). *Conference Ranks: Lookup the Rank of Your Conference*. [Online]. Available: <http://www.conferenceranks.com/>



**ADEL REZAPOUR** received the B.S. degree in software engineering from the Hatf Higher Education Institute, Zahedan, Iran, in 2010, and the M.S. degree in software engineering from Islamic Azad University, Birjand, Iran, in 2016, where he is currently pursuing the Ph.D. degree in software engineering. His research interests include network security, intrusion detection and response systems, alert management, machine learning, and optimization problems.



**MOHAMMAD GHASEMIGOL** is currently a Research Assistant Professor with the School of Cybersecurity, Old Dominion University. Before, he was a Research Assistant Professor with the University of North Dakota and an Associate Researcher with Imperial College London. He has been an Assistant Professor in computer engineering with the University of Birjand, since 2016. His research interests include the various aspects of AI, machine learning, and cybersecurity including incident handling, intrusion detection and response systems, insider threats, alert management, clustering and classification methods, deep learning, safe learning, explainable AI algorithms, and data analysis.



**DANIEL TAKABI** (Member, IEEE) is currently a Professor and the Director of the School of Cybersecurity, Old Dominion University. Prior to this, he was the Founding Director of the Information Security and Privacy: Interdisciplinary Research and Education (INSPIRE) Center, designated as the National Center of Academic Excellence in Cyber Defense Research (CAE-R), Georgia State University. His research interests include the various aspects of cybersecurity and privacy, including trustworthy AI, privacy-preserving machine learning, adversarial learning, advanced access control models, insider threats, and usable security and privacy.

• • •