sciendo

JAISCR, 2021, Vol. 11, No. 2, pp. 111 – 142
10.2478/jaiscr-2021-0008

A SURVEY ON MULTI-AGENT BASED COLLABORATIVE INTRUSION DETECTION SYSTEMS

Nassima Bougueroua[1], Smaine Mazouzi[1], Mohamed Belaoued[1], Noureddine Seddari[1], Abdelouahid Derhab[2], and Abdelghani Bouras[3]

[1]*Department of Computer Science, 20 August 1955 University of Skikda, Algeria*

[2]*Center of Excellence in Information Assurance (COEIA), King Saud University, Riyadh, Saudi Arabia*

[3]*Department of Industrial Engineering, Alfaisal University, Riyadh 12714, Saudi Arabia*

[*]*E-mail: bouguerouanassima@gmail.com*

Submitted: 23th June 2020; Accepted: 6th October 2020

Abstract

Multi-Agent Systems (MAS) have been widely used in many areas like modeling and simulation of complex phenomena, and distributed problem solving. Likewise, MAS have been used in cyber-security, to build more efficient Intrusion Detection Systems (IDS), namely Collaborative Intrusion Detection Systems (CIDS). This work presents a taxonomy for classifying the methods used to design intrusion detection systems, and how such methods were used alongside with MAS in order to build IDS that are deployed in distributed environments, resulting in the emergence of CIDS. The proposed taxonomy, consists of three parts: 1) general architecture of CIDS, 2) the used agent technology, and 3) decision techniques, in which used technologies are presented. The proposed taxonomy reviews and classifies the most relevant works in this topic and highlights open research issues in view of recent and emerging threats. Thus, this work provides a good insight regarding past, current, and future solutions for CIDS, and helps both researchers and professionals design more effective solutions.

Keywords: IDS, CIDS, MAS, Artificial Intelligence

1 Introduction

Nowadays, our computer networks and mobile devices are facing an unprecedented and a massive number cyber-attacks (intrusions, malware, etc.), causing billions of dollars of losses every year. Indeed, according to the latest global statistics[1] published in March 2020, there were more than two billion intrusion attempts in 2019. According to D.Denning and P.G.Neumann [46], an intrusion could be any attempt by a user to change work tasks, acquire new skills, or make typing errors; updates software; or change the workload on the system and cause loss of confidentiality, loss of integrity, or an authorized use of resource.

Network intrusion attacks can take several forms, such as network traffic flooding, buffer overflow attacks which allow executing a set of malicious commands, as well as protocol specific attacks, when hackers target a network through a se-

[1]http://www.internetworldstats.com/stats.htm

curity vulnerability. The most common types of network attacks are:

- Denial of Service (DoS) Attacks such as: TCP/SYN Flooding [49], Buffer Overflow Attacks [41].
- Distributed Denial of Service (DDoS) attacks such as: ICMP Tunneling Attacks [167], Scanning Attacks [191], Traffic Flooding[198], and Asymmetric Routing [130].
- Malware (e.g. Trojans, Worms and Virus, etc.) [17, 15].

There is a high need to develop more effective security systems that provide a high level of protection to systems and networks against attacks. For more protection of computers and networks, we can set up an intrusion detection system (IDS) [2, 148]. Many limitations of this approach are found with regard to the sophisticated attacks mentioned above [185]. For this reason, researchers have shifted from monolithic IDS towards collaborative and real-time one [185, 94] in order to reduce the computation cost by sharing IDS resources between network nodes and minimize the number of false alarms generated by isolating IDS [201, 114]. Thus, and in order to support this new generation of IDS, new paradigms were adopted such as multi-agent systems (MAS) ones, which are one of the paradigms that are better adapted to the definition of intrusion detection in collaborative networks [83, 50, 4].

Moreover, other artificial intelligence (AI) techniques can be combined with this paradigm to make agents and MAS more suitable for intrusion detection task [83]. The main contributions in this survey can be summarized in the following points:

- We present a clear taxonomy that allows to classify the existing work based on three factors: the architecture of the CIDS (centralized, hierarchical and decentralized), the agent technology (mobile, situated and reactive) and many decision techniques;
- A detailed description of related works that provided CIDS modelled agent;
- Despite the fact that MAS is a quite old technology, it has still a great popularity and is applied. It remains a very useful in several domains in recent years [48, 81, 119, 16];
- We focus on both past and current cutting edge technologies, such as Deep Learning;
- Finally, we identify challenges, future directions, and open issues that help researchers to design more efficient MAS-based CIDS.

This paper is organized as follows: in the 2 Section, we introduce some basic concepts about IDS and CIDS. In the 3 Section, we present a comparison of our survey with existing ones that deal with similar topic. The 4 Section is dedicated to the proposed taxonomy of collaborative intrusion detection systems, where we will review the most recent related work. In Section 5, we provide a detailed discussion of the proposed taxonomy, as well as the open issues and future directions. Finally, Section 6 concludes our work.

2 Background

2.1 Intrusion Detection Systems (IDS)

Historically, IDS were instantiated in the 80s [185]. An intrusion detection system can be defined as a tool that analyzes the activity of a system or a network to detect any action that compromises the integrity, confidentiality, or availability of resources that can be attacked by an intruder [2, 148]. An intrusion detection system has three main components which are [99]:

- Monitoring component: Allows monitoring of local events and neighbors as well as the use of resources;
- Analysis and detection component: The main component that is used to decide whether an event is an attack or not, after the analysis of the network activity;
- Alarm component: Generates alarms when attacks are detected.

Intrusion detection systems can be broadly classified into two categories, which are: misuse-based IDS, and anomaly-based IDS [189]. Misuse detection relies on previously well-known attack signatures that are stored in a dedicated database [112]. Anomaly detection, on the other hand, relies on

defining a normal behavior profile, and then any deviation from this profile is considered as an attack [140]. Anomaly detection has some major drawback, namely: it suffers from high false alarms rate compared to misuse detection [89, 140]. Note that a false alarm, also called a false positive, occurs when the detection system reports an event as an intrusion while it is a legitimated activity [140], at the opposite of a false negative, which arises when a malicious activity is not detected as an attack [140]. Despite its high level of false alarms, anomaly detection allows to detect new attacks for which signatures are not yet defined [143]. This is the main advantage of this class of IDS.The com bination of the two categories, by taking into account their respective advantages, allows to obtain better hybrid intrusion detection systems that can be used to detect both known and unknown attacks [178].

According to their location, IDS can be also classified as Host-based (HIDS) and Network-based (NIDS). A HIDS is a system that collects and displays information from an audit data source and is located on a single host, and thus, attacks are detected at this host level [131, 161]. Primarily, it monitors and analyzes the internals of a computer, node or device activity [45]. Nowadays, it can be also used to monitor network [138]. Historically, the first security systems where HIDS-like[79]. On the other hand, a network-based intrusion detection system (NIDS) is an IDS that monitors and analyzes the network traffic for a better protection against intrusions [131, 135, 199]. It reads and examines incoming packets, and intrusions are detected, the IDS notify administrators or forbids the involved IP source address from accessing the network [131]. According to [197], regarding their location, NIDS can be set up in three of common placements, which are directly connected to a switch spanning port [34], using a network tap, or connected inline [139].

According to [116], in addition to HIDS and NIDS, IDS can be classified into three other classes: WIDS (Wireless IDS), NBA (Network behaviour analysis) and MIDS (Mixed IDS), depending on where they are deployed to detect suspicious activities and the types of events they can identify:

- WIDS: captures and analysis wireless network traffic.
- NBA: controls the network traffic in order to detect attacks with unexpected traffic flows.
- MIDS: allows implementing several technologies, for more complete and more precise detection.

Another classification [197] regroups IDS in two categories according to the manner IDS respond during an attack: passive and reactive (active) systems. Passive IDS identify possible security breaches, logs information about them, trigger alarms, and send reports to the security administrators that are outside the network [197]. Active IDS, which are also known as IPS (Intrusion Prevention Systems), automatically take action on detecting any possible security threats, and they are placed inline in a network [197].

Classical IDS have many drawbacks such as:

- Usually, classical IDSs suffer from a high false alarms rate which results in a low detection accuracy, and in the case of a large scale network with a large number of users, the number of false alarms is exponentially increasing, despite changes to the IDS' settings [87, 128].
- Despite the improvement in classical IDSs over the past years, they can still be bypassed by sophisticated attacks such as Advanced Persistent Threats (APTs) [123, 38], Distributed Denial of Service (DDoS) [86, 134], etc.
- Classical IDSs do not process encrypted packets, which can allow the intrusion of the networks [195, 104].
- Classical IDSs provide security logs and alerts based on the network address associated with the IP packets being sent over the network. Therefore, if the address contained in the IP packet is spoofed, the IDS manager will not be able to stop intrusions on the network [85].

Seeing the limitations of IDS, described above, mainly due to the fact that classical IDS work in an isolated way, computer security researchers have shifted to Collaborative Intrusion Detection Systems (CIDS).

2.2 Collaborative Intrusion Detection System (CIDS)

Recently, some authors attempted to overcome the limitations of existing IDS technology by introducing the concept of collaboration. It is based on sharing data and/or resources between nodes and coordinating them in order to improve the security of networks or an entire system [126, 160, 114]. The collaborative approach proved its effectiveness in detecting vulnerabilities and analyzing security, predicting attacks, and protecting sensitive information, as well as for its ability to address the challenges of traditional security [126, 160, 16, 114].

In 1991, Snapp [169] proposed the first Collaborative Intrusion Detection System (CIDS). It consisted of a prototype in which nodes collaborate to detect intrusions. Spafford [171] defined a CIDS as: "A system where the analysis of the data is performed on a number of locations proportional to the number of hosts that are being monitored".

In a wide area network, CIDS collect and correlate audit data from different hosts. These hosts communicate with each other and use a NIDS and/or a HIDS, in addiction to both misuse and anomaly based detection techniques to take advantage of their benefits [95].

As denoted by A.Jones in [95], a collaborative IDS generally use a central analyzer that scrutinizes data received from other IDSs in the network. Monitoring and collaboration in network pose some new requirements [90], namely:

- CIDS must provide mechanisms that allow the network to produce a large amount of data;
- In large networks, CIDS should provide some means for determining where to look for events;
- Scalability, since it must interoperate with other CIDSs (hierarchical architecture).

A CIDS should generate a minimal amount of traffic on the network, and therefore, should process local event data [186]. Moreover, it has been noted some limitations and challenges of CIDS. For instance, the central server (unit) is considered as a single point of failure and at the same time requires high communication and processing capabilities [10]. CIDS also suffer from high false positive rates (low detection efficiency), as well as limited flexibility, and limited response capability [90].

MAS have autonomous and cooperating agents distributed throughout its system environment which carry a certain number of characteristics such as situation, intelligence, autonomy, flexibility, and cooperative problem-solving abilities [96]. MAS are used to solve complex problems involving decentralized data and their tasks are distributed over a number of agents [163]. The workload is distributed and data analysis is done quickly, thus MAS can reduce system complexity and software costs [163]. Furthermore, MAS are the most appropriate paradigm to attain the objective in collaborative systems [43]. It has been reported in several works that collaboration within distributed entities can be well performed using multi-agent systems (MAS) [50, 4].

In such systems, agents play different roles aiming at improving the performance of the overall detection system. This will be the focus of our work, namely, providing a taxonomy for MAS-based collaborative intrusion detection systems.

3 Existing surveys

In this Section, we review the main surveys in the field of CIDS and MAS, the topics they covered, and then we compare them with our work in order to highlight our contributions.

Meng et al. [126] provided a general framework for collaborative security, including intrusion detection, anti-spam, anti-malware and botnet detection. The classification of existing CIDS is based on three factors: communication, robustness, and privacy. In addition, they have posed several challenges with the current structure of collaborative security systems and provide a platform on which future research on this type of security system can be based.

The work of [183] is a detailed study of the current CIDS following the classification into centralized, decentralized, and distributed CIDS. Based on the identified requirements and building blocks, the authors summarize attacks for the CIDS evasion and attacks on the availability of the CIDS themselves. The solutions presented are discussed with the defined requirements and building blocks, as well as possible attacks.

Tiwari and Gour [179] provide a survey on the CIDS-based mobile agent where only log file base collaborative IDS system is considered. They also include different challenges and the best solution with mobile agent. This survey helps the user to select appropriate IDS.

Folino and Sabatino [59] make a brief review on ensemble based IDS with a high-light on the collaboration and distribution approaches and provide applications and challenges with references for further studies.

Othman et al. [137] review different types of IDS related to different environments and platforms through comparative approach. Also, they present a classification of IDS types based on criteria and introduces features of each types.

In Table 1, we illustrate gap analysis to compare between the previous related surveys and ours.

On the basis of the conducted gap analysis presented in Table 1, we can see that our survey outperforms the other surveys by providing a broader coverage of the aspects and technologies involved in the construction of collaborative IDS. If we take as a reference the survey of Dorri et al. [48] that provides a comprehensive discussion of all aspects of MAS, including their types, our work has covered three different types of agents while other surveys discussed at most one type of agents. Moreover, and regarding the decision techniques criteria, our survey is the only one that considered nine (09) different techniques, much better than what others do see Table 1. Finally, to the best of our knowledge, this is the first work that has been entirely dedicated to MAS-based collaborative intrusion detection.

4 A Taxonomy for multi-agent based CIDS

When designed according to new approaches or using emergent technologies, a collaborative intrusion detection system has certain specific characteristics. In this Section, we provide the current state of the art of the field, by introducing methods used for constructing CIDS, with a particular focus on collaboration methods that integrate multi-agent systems [60]. We will split these methods into three principal categories, namely: the architecture, the used agent technology, and the decision technique. Figure 1 illustrates the suggested classification (taxonomy).

4.1 Architecture

Collaborative intrusion detection systems are mainly designed according to two main types of architectures: centralized and distributed. However, another intermediary architecture type called hierarchical is identified and is considered as a hybrid one. Thus, in this paper, we extend the CIDS classification according to three types of architectures, namely: centralized, distributed, and hierarchical.

4.1.1 Centralized

The centralized CIDS are considered, by some authors, as not truly distributed systems, because of the centralized data analysis [25]. They are usually composed of monitoring units and a central control unit, where the monitors send intrusion data to the controller for analysis [36], as illustrated in Figure 2. This generates additional load on both controller and network, causing network congestion [36]. Such systems can be compared to conventional IDS, with the capability to be connected to remote devices [169]. So, security data are collected into the central device and then analyzed [169]. In addition to bandwidth overcapacity, adding a new device requires intensive maintenance labor [169].

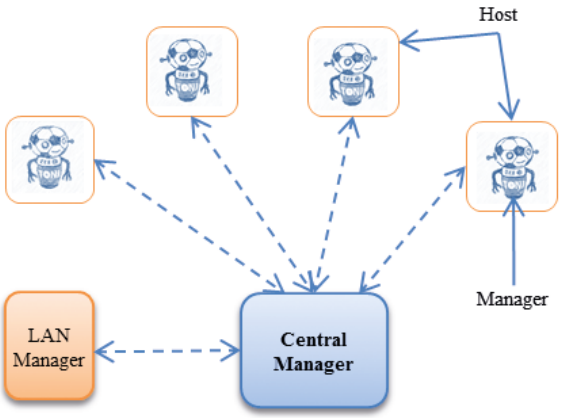


Figure 2. Architecture of centralized control of a Collaborative Intrusion Detection system

For instance, the collaborative IDS NetSTAT [186] suffers from non-scalability and is limited by its centralized nature. Also, [169] proposed a centralization CIDS that have many drawbacks, such as:

Table 1. A gap analysis of existing surveys that focus on the use of multi-agent systems in intrusion detection: ✓: Topic is covered, ✗: Topic is not covered
C: Centralized Architecture, **H**: Hierarchical Architecture, **D**: Decentralized Architecture
SA: Situated Agent, **MA**: Mobile Agent, **RA**: Reactive Agent, **CA**: Cognitive Agent, **HA**: Hybrid Agent
ES: Expert System, **NN**: Neural Networks, **BN**: Bayesian Networks, **SVM**: Support Vector Machine, **DT**: Decision Tree, **DL**: Deep Learning, **GA**: Genetic Algorithm, **GrA**: Greedy Algorithm, **PSO**: Practical Swarm Optimization

Surveys	**Covered Architecture of CIDS**			**Covered MAS aspects of CIDS**					**Covered Decision Techniques of CIDS**									
	C	H	D	SA	MA	RA	CA	HA	ES	ON	NN	BN	SVM	DT	DL	GA	GrA	PSO
[179]	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
[183]	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
[59]	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓
Our Survey	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗

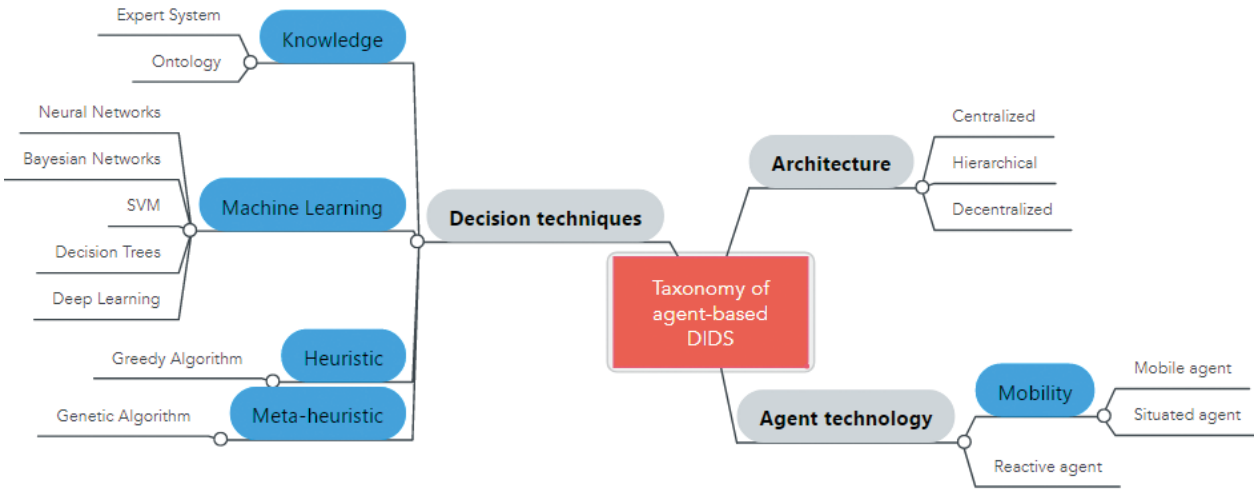


Figure 1. The proposed taxonomy of CIDS

– Communication with the central manager component generates an overload of network traffic;

– Some of existing IDS architectures require a platform with specific components;

– When the central device is out of service, the system stops, and the network is entirely not protected against attacks.

4.1.2 Hierarchical

Even when using traditional communication schemes, CIDSs can be more scalable when agents are hierarchically organized [42]. According to this architecture, agents collaborate and share their data according to a hierarchical structure. Thus, agents at the lowest level of the hierarchy are dedicated for traffic analysis [162]. However, agents at the higher-level analyze advanced data received from several lower-level agents and try to establish an overall view of the system state regarding security aspects [162].

The hierarchical model allows significant benefits in scalability, flexibility, extensibility, fault tolerance, and cooperation [162]. However, such an architecture has two principal drawbacks, which are:

– As data analysis is centralized at the top levels of the hierarchy, that makes the system not fully distributed [72].

– The nodes that are the closest to the root node suffer from low fault tolerance and overhead vulnerability [106].

In [171], Spafford proposed AAFID, a hierarchical collaborative intrusion detection system where agents belong to several levels. At the lower levels, agents collect and analyse data, and at the higher levels, agents, which play the roles of transceivers and monitors, produce an overall view of the activities and establish global decision of detection.

In [6], El-ajjouri suggest a novel approach for collaborative intrusion detection with a hierarchical scheme split into layers that are: the monitoring layer, the classification layer, and the administration layer. In each layer, various agents collaborate to detect intrusions. The combination of Multi-Agent System (MAS) and Case-Based Reasoning (CBR) techniques offer an intelligent intrusion detection system that is able of learning and reasoning. Therefore, the proposed architecture has superior scalability. Moreover, the decentralization of the system, makes it possible to improve treatments and minimize the overload of the network.

A new approach for collaborative intrusion detection based on mobile agents was suggested by Li [115]. The latter, which can be considered as a hierarchical approach, does not have a single point of failure like most of the existing methods. Moreover, the experimental results have shown that the proposed approach has a good detection performance.

4.1.3 Distributed (decentralized)

According to recent researches, the collaborative architecture is the most suited for decentralized systems, especially in complex systems where there is a high number of interacting entities, and where decisions at a high level, emerge from interactions within low level entities [156]. For decentralized CIDS, it is required to install a security manager on each host of the network, managers collaborate to detect intrusion attempts [7]. In such systems, scalability is a great challenge, mainly when there is a large number of security managers [106]. The collaborative structure has no single point of failure and it is more scalable [92]. However, the fact that there are many information pathways that are unnecessary is the main drawback of a such scheme[92]. The Cooperating Security Managers (CSM) is a good example of collaborative IDS that uses a decentralized architecture, based on the principal cited above [58].

Authors of DIDMA [98] introduced decentralized CIDS using mobile and static agents in order to improve detection capabilities and to make the system more scalable. Mobile agents perform the task of aggregation and correlation of intrusion data received from static agents in a decentralized manner.

In recent years, collaborative architecture remains in the interest of several works [100, 154, 121, 78, 202]: for their robustness and scalability, compared to centralized architectures. In a collaborative system, removing the central entity results in peer to peer (P2P) organisation, where no more privileges are accorded to any entity regarding others [157].

The application of P2P in large scale causes the problem of the efficiency in location and rooting [157]. Thus, computer scientists have designed novel solutions, where a massive set of entities interact to accomplish the whole function of the system [157]. In theory, in an approach using a P2P network, each node must collect, analyse and elaborate alarms, and finally share the final results globally [59]. Oriola in [136] introduced a platform that uses the principle of P2P based computing to improve intrusion detection in distributed networks systems. So, several benefits can be observed like: there is no central coordination, equivalent rights between entities in the network, robustness, several resources can be shared, scalability and there is no single point of failure. However, P2P has some challenges like insider menace detection, threat detection and vulnerability, low intelligence, and absence of evidence.

In Table 2, we summarize the main studies, reviewed according to the architecture-based classification.

4.2 Agent Technology

Ferber [56] has defined an agent as a computational or physical entity placed in a virtual or real environment, perceives and communicates with other agents. Additionally, it is animated by inner inclinations (goals, beliefs, etc.), and it has an autonomous behavior, which is the consequence of its perception, illustration, interaction, and communication with the environment and with other agents [56]. We can identify the following types agents:

- Static agent: always located in the same position in the environment and is able to act on it [201];
- Mobile agent: can move around in the environment and can be hosted by other agents [201];
- Reactive agent: perceives its environment and responds to changes that occur there. Reactivity also means the ability of an agent to alter its behavior when environmental conditions change;
- Cognitive agent: able to find a solution for a complex problem while communicating with other agents and interacting with its knowledge base [23].
- Deliberative agent: is one who has an explicit representation, symbolic of the word, and in which decisions are made via symbolic reasoning [192].
- Hybrid agent: has the characteristics of reactive and cognitive agent. These agents have a reaction revolution to the resolution of known problems, they also have a cognitive attitude in the complex situation of the system [23].

The following aspects enable agents to solve complex tasks:
Autonomy: the agent can independently execute the decision making process and take appropriate action. Thus, the agent is not guided by the outside, but by his tendencies [56, 23].
Flexibility: can be seen as a form of intelligence. being flexible means that the agent is [93]:

- Sociability: agents can share their knowledge and request information from other agents to improve performance in achieving their objectives and help others in their activities.
- Pro-activity: Each agent uses its history, sensed parameters, and information of other agents to predict the possible future actions.
- Reactivity: the agent must be able to perceive his environment and respond in time to changes that may affect this environment.

Adaptability: an adaptive agent is an agent capable of controlling his abilities according to the environment in which he evolves and according to the agent with which he interacts [56].

The real advantage of agents can be exploited when they work together with other agents to solve a complex task and they are called multi-agent systems (MAS) [201]. We have discussed sociability in the aspects of agents, but in reality, this property is centered on the interactions between agents in MAS. Thus, sociability involves different properties, such as cooperation, coordination, delegation and communication [48]. MAS resolve problems in a collaborative manner, which makes it more reliable. Thus, the task can be reassigned to another agent if the first fails [48]. In fact, MAS is an effective solution to solve complex problems thanks

to its characteristics such as low cost, efficiency, reliability, etc. Moreover, to solve a complex problem in MAS it must be divided into several smaller tasks, each of these tasks being assigned to a separate agent[151]. This part of our paper describes a framework for collaborative intrusion detection using agent-based technology. Agents are ideally qualified to their mobility, reactivity, and their situation.

4.2.1 Mobility

a. Mobile agent

Funfrocken [62] states that "Mobile agents are programs that operate continuously and are able to learn and move from host to host to gather information to fulfil a task on behalf of a user".

The use of mobile agents can decrease the network load and overcome latency; they also make the system more scalable [180]. The environment of Mobile Agents (MAs) is a software system, distributed on heterogeneous computers connected to a network, offering an environment of execution [73]. The mobile agent environment may provide services that [73]:

- Support service which relates a mobile agents to their environment;
- Related to the environment on which mobile agent was built;
- Make interact with other mobile agents;

In Figure 3, the environment of mobile agents is built so mobile agents travel between hosts and the communications between all elements of the system can be shown by bi-directional arrows [73]. The approaches using mobile agents allow designing efficient collaborative IDS, especially when taking advantage of the benefits of mobile agents [51].

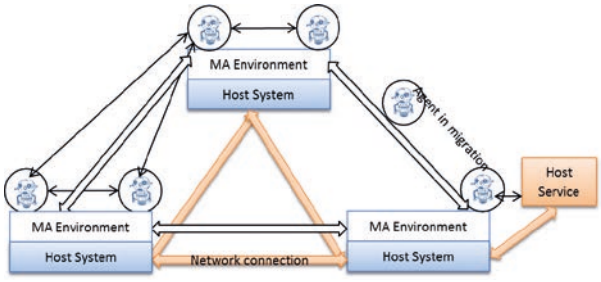


Figure 3. Environment of mobile agents

Eesa et al. [50] propose a novel CIDS based on the combination of Cuttlefish Optimization Algorithm (CFA) and Decision Tree (DT). The system contains Collector Mobile Agent (CMA), Rule and Feature Generator Agent (RFGA), Controller Agent (CA), Action Mobile Agent (AMA), User Interface Agent (UIA), and Several Nodes (SN) (local networks) each with Sniffer Agent (SA) which interact with the server. The RFGA agent generates a subset of features to reduce the amount of data and find an optimal subset of features; while DT is used to measure the selected features. In this model, the criteria used for KDD Cup 99 are the Cost Per Test (CPT) which is calculated by a confusion matrix, and a given cost matrix [53]. The experimental results show that the proposed system gives a better performance and the implementation of different techniques also provides clues to create more effective intrusion detection models.

Li et al. [115] propose a new CIDS method based on the mobile agent, who benefits from the agent's characteristics: intelligence and mobility. Moreover, the proposed method has many positive characteristics:

- Improves real-time capacity;
- Solves the problem of bottlenecks;
- No single point of failure;
- Robustness and fault tolerance;
- Decrease in the rate of false positives;
- High rate of true positives;
- The effectiveness of profile classification.

The new approach suggested by Riyad [154], which is an adaptive collaborative intrusion detection system architecture using multi agents. The system is fully distributed without a central point of failure, the use of mobile agents considerably reduces the false positive rate and facilitates the identification of distributed attacks. The results show that the system is more scalable and efficient.

b. Situated agent

In situated multi-agent systems, the environment has a low importance in modelling systems and

phenomena [190]. Moreover, agents and environment are complementary, and the environment is both a mean of communication and a subject on which agents operate [190]. They mutually affect each other during their evolution to achieve a global goal [190]. A generic model presented in Figure 4 shows how a situated agent makes a decision and interacts with the environment.

Some characteristics of situated agents, which make them powerful and suitable for intrusion detection, are listed below [190] :

- Intelligence is produced from the interactions and also from the capabilities of individual agents;
- Situated agents usually communicate indirectly via the environment;
- To set up explicit collaborations, reflected in mutual commitments, the agents need to communicate directly;
- Situated agents select actions based on internal stimuli and stimuli perceived in their environment.

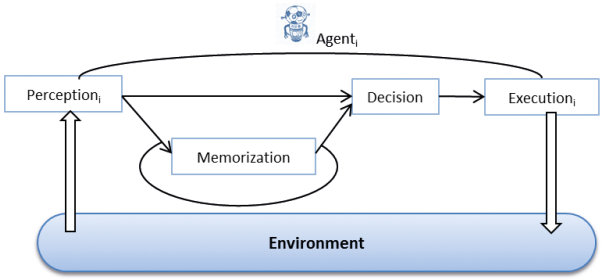


Figure 4. Generic model for situated agents

Nafir et al. [133] proposed a collaborative intrusion detection system based on situated agents technology. The proposed CIDS is based on a collective approach for collaborative detection of DDoS attacks in wide area networks. An agent, which plays several roles, is situated on each node of the network. The agent can perform the task of a local intrusion detection system. Moreover, the agent ensures the exchange of security data with its neighbors by collecting information on attacks using local event frequencies of neighboring agents and computing a global event frequency. Next, it will reach a local decision, and finally a global one. The results of simulations show that the proposed system was able to improve the detection rate. Moreover, the system adopts the negotiation and the decision propagation to solve the problem of false alarms.

4.2.2 Reactive agent

Usually, reactive agent reacts rapidly for problems that do not need complex and difficult reasoning [23]. Thus, the intelligence of the system emerges from the interactions among many of this type of agents [23].

According to Bornscheuer [21], Intelligent behavior consists of reactive behavior, reactive reasoning depending on current beliefs which are dynamically updated by reflective reasoning. As shown in Figure 5, the reactive agent perceives and acts in its environment through reactive reasoning.

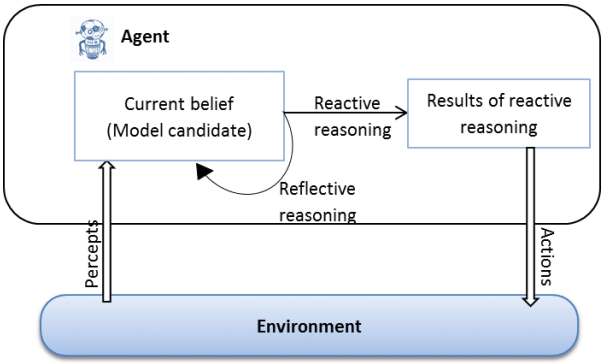


Figure 5. Reactive reasoning of a reactive agent

The authors of [4] suggested a MAS-based CIDS which combines two categories of agents namely: reactive and mobile agents that communicate and cooperate to make the MAS-based CIDS more efficient and secure. The results show that the suggested system increases the detection rate, reduces false positives, and detects known and unknown attacks in a cloud computing environment.

4.3 Decision Techniques

Most existing detection systems are arranged likewise signature-based or behaviour-based. In either case, one each system decides based on the data it holds. Therefore, knowledge-based, machine learning techniques and meta-heuristics are the most used techniques. In this review, we tend

to introduce the most utilized techniques, and how they were used, in addition to related work published in the literature.

4.3.1 Knowledge

As denoted by T.R.Gruber [75]: A conceptualization is an abstract and simplified vision of the world that we wish to represent for some specific purpose. Each knowledge base or knowledge-based system or knowledge-level agent is committed in a conceptualization, explicitly or implicitly. Knowledge representation is based on a conceptualization which is a composition of objects, concepts, other entities, and the relations that exist between them [70]. In the next part of our survey, we will represent expert and ontology-based systems used as decision mechanisms in CIDS.

a. Expert Systems

Expert Systems (ES) are a Section of Artificial Intelligence (AI), developed by the AI community in the mid-1960s [181]. The main idea of using ES is simply that expertise, i.e. the whole task-specific knowledge, is transmitted from a human to a computer [70]. Expert systems offer powerful and flexible ways to get resolutions to a diversity of problems that often cannot be addressed by traditional methods[181]. ES include three main elements, which are: the knowledge base, the inference engine, and the user interface [12, 88, 107] as showed in Figure 6:

– Knowledge base uses different knowledge representation techniques, mainly production rules;

– The inference engine is active through a consultation session. It examines and manages the status of the knowledge base, and finally defines the order in which inferences are made;

– The user interface element allows communication between the system and the user. It mostly includes screen presentations, a consultation/advice conversation, and an explanation element.

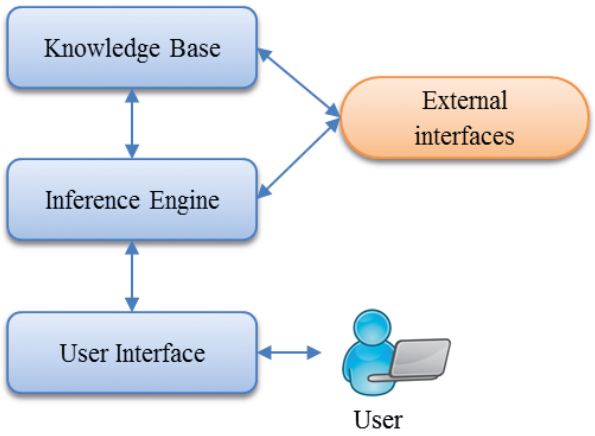


Figure 6. Expert system architecture

Some researchers have used expert systems to build IDS. It was an important step in the development of more effective security systems based on anomaly detection [32]. Expert systems require frequent updates that must be performed by a system administrator[32]. If the administrator ignores updates or seldom runs them, it will lead to an expert system with reduced efficiency that degrades the security of the entire system [32].

In [169], the authors proposed a rule-based expert systems CIDS, which combine multiple IDS running individually to detect wide-network intrusions. A single host monitor per host and a single LAN monitor for both broadcast LAN segments in the observed network. Each local intrusion detection system collects any information on suspicious events locally and converts it to a homogeneous format. Then, it reports the generated alerts to a centralized rule-based expert system for more evaluation. Alerts are produced if any rule has been satisfied after correlation. Nevertheless, smart intelligent attackers can evade such CIDS by reducing the attack traffic for a given network. The proposed prototype is also applicable to the small network of a single computer. The prototype has proved the viability of distributed architecture in resolving the network-user identification problem. Nonetheless, there is no real analysis of network activity patterns; and aggregation is used only to track users who use multiple account names as they move around the network.

b. Ontology

According to T.R.Gruber [76]: "An ontology is an explicit specification of a conceptualization. Therefore, it must define a set of representational terms to describe the ontology of any program"

In ontologies, descriptions associate the names of entities in the space of discourse like classes, relations, functions, or any other objects with human-readable text illustrating what the names are meant to represent, and formal axioms that restrain the interpretation and well-formed use of these terms [27]. Thus, the ontology is designed to allow sharing and reuse of knowledge between entities of the same field [27]. RDF-S (Resource Description Framework-Schema) provide a visualization service for ontologies and knowledge representation of any object [24]. The RDF is a model and defined as a set, called Resources, Literals, Properties (subset of Resources), and Statements, where every element is a triplet of the form: subject, predicate, object [27, 122]. Predicate is a member of Properties, subject is a member of Resources, and object is also a member of Resources or Literals [27]. Few approaches and works in the field of intrusion detection are dedicated to the integration of the ontological model with the IDS [24]. In order to improve the accuracy and efficiency of detection and to make intelligent reasoning, the approaches are adapted to the trend of collaborative IDS mixed with an ontological structure [24, 145].

In [1], Abdoli and Kahani described CIDS that extract semantic relations between attacks using a particular ontology. The purpose behind using ontology is to provide a mean of extracting semantic relations between attacks and intrusions alerts produced by diverse IDS. The proposed system is a network that comprises IDSagents and a special MasterAgent which contains the proposed attack ontology. Whenever an IDSagent detects an attack or a novel suspicious condition, it sends a detection report for the MasterAgent. Therefore, the latter extracts the semantic relationship between computer attacks and suspicious situations in the network with the proposed ontology. The simulation was implemented using the KDD Cup99 intrusion detection data-set and was measured by Cost per Example (CPE), false alarm, and detection of DoS attacks. In addition, the use of the ontology model allows reduction of costs of false alarms.

Authors of [26] proposed an architecture aiming to enable knowledge sharing and improve reuse between entities within a domain by implementing ontologies. In this system, all entities are considered as agents that are assigned to different functions: Monitor Agent, Analysis Agent, Executive Agent, Manager Agent, and Knowledge Base. The latter includes:

- Attack Ontology: has data properties that represent the attributes of a connection.
- Instances: contain data pointing to a particular attack.

For the detection of an attack, the same ontology is taken into account in each IDS. Consequently, this system reduces the resources usage overload and it is more optimized.

4.3.2 Machine Learning (ML)

As stated by Kotsiantis et al. [102]: Machine Learning is the search for algorithms that reason from externally supplied instances to produce general hypotheses, which then make predictions about future instances".

ML techniques that have been widely utilized in the construction of CIDS are Neural Networks, Bayesian Networks, support vector machines, decision trees and deep Learning.

a. Neural Network

An artificial neural network (ANN) is the widely used machine learning technique for solving classification problems [44]. An artificial neural network is a set of highly interconnected elements, which are able to transform data from input and produce results at output [61, 80]. Results are obtained according to the characteristics of the elements themselves and the weights of links between neurons [61, 80]. By adjusting connection weights between the nodes, the network is able to adapt the expected results taking into account the inputted data [61, 80]. Artificial neural networks have the ability of learning and generalizing from limited, noisy, and incomplete data [193]. They have, hence, been successfully employed in broad spectrum of data intensive applications [193]. The neural networks are one of the main soft computing systems [33, 54, 111, 159, 174, 71]. It has been successful

in resolving many issues and many authors have benefit from the advantages of applying neural networks to IDS [33, 54, 111, 159, 174, 71, 141]. The latter can use ANN model that utilizes the artificially created anomalous-behaviour feature values to detect probable intrusions into the network [11]. Most of these neural network applications use a single neural network structure, which has only one set of input, output, and hidden layers [127]. There are two principal drawbacks that appear in a single neural network structure [127]:

– Firstly, all nodes of the network depend on each other. If its input data have any changes, the complete system has to be retrained.

– Secondly, the neural network will become progressively complex if more variables and hidden layers are introduced.

Shosha [165] developed a Collaborative Intrusion Detection System based on community cooperation between agents of anomaly detectors to identify abnormal behaviors in SCADA networks, using Feed-Forward Artificial Neural Networks classifiers. It is able to detect well-known attacks at both the control center and substation levels. In the test phase of the proposed system, two attack-scenarios were used: the first is to attack the SCADA substation on four different intelligent electronic devices with fake IP addresses. The second is an attack that aims to damage the control center of four substations controlled by IP. The proposed CIDS achieved a good detection rate while minimizing false positives.

Bukhtoyarov and Zhukov in [28] present a distributed architecture of IDS which use ensembles of neural networks. The implemented system uses a probabilistic approach for the generation of a neural network on every node of a network. Next, the neural networks are combined in an ensemble, using genetic programming. Afterwards, every node classifies the traffic independently from the other nodes and it inquires the ensemble only within the case in which it is "not confident" of its prediction. The "confidence" threshold characterizes the range of values at the output of a single neural network classifier, as well as the emergence of the uncertainty situation. In other words, an agent cannot identify a class for a specific reason with sufficient confidence. Thanks to some properties of neural networks, there are reasons to trust the solution of ensemble classifier more than the solution obtained with one agent. Experimental results confirm the high efficiency of the security system based on ensemble-distributed classifiers. The approach was also tested on a KDD Cup '99 data-set in terms of Detection Accuracy and False Positive Rate.

Authors of [166] proposed a multi-agent-based collaborative IDS (CIDS) model based on Backpropagation neural network. This model adopts the modes of collaborative detection and distributed response, where agents were relatively independent. The advantages of the proposed system are: reduce the mobile data process, load equalization, good error-tolerating, and effective collaborative intrusion detection. The system was tested on the KDD Cup 99 data set, and the results show that the system could improve the efficiency of detection accuracy and significantly reduce the workload of the center console.

b. Bayesian Network (BN)

According to Heckerman [82]: *" A Bayesian network is a model that encodes probabilistic relationships among variables of interest. Actually, it is a procedure that produces numerous benefits as well as capability of encoding interdependencies between variables and predicting events, in addition to the ability to incorporate both prior knowledge and data"*

However, as indicated by Kruegel[105], a serious inconvenient of implementing Bayesian Networks is that a computational effort is required and extensively higher and their results are similar to those derived from threshold-based systems. The idea of using Bayesian Networks in Intrusion Detection Systems has come to combine different anomaly measures to get better results in detecting intrusion [29]. BN is an appropriate representation to solve a problem [29]. Moreover, BN is a probabilistic graphical model that represents a set of variables and their conditional dependencies via a Directed Acyclic Graph (DAG) [40]. DAG can efficiently encode the joint probability distribution for a larger number of variables, and DAG's arcs represent causal dependence between the parent and the child [29]. It is composed of nodes (variables) and directed edges arrows between nodes [74].

In [30, 13], the authors suggested collaborative architecture for IDS that support Bayesian networks, but they use traditional probability update approaches for Bayesian networks and are restricted.

Rezaul et al. [152] proposed a new study that applied Bayesian technique in the field of CIDS to improve the efficiency of the detection mechanism for mobile ad-hoc network. Experimental results improve that the proposed system is more evident, with very low false positive rate and efficient detection of intrusions. The system has better performance in comparison with other work.

Fung et al. [64] have designed a trust mechanism based on challenges for Collaborative Intrusion Detection Networks where all agents act selfishly to achieve their individual goals in which the confidence of a node can be determined based on the answers given to the challenges involved. Their model guarantees both confidence and trust estimation. In the first proposed work in [63], they proposed a collaborating Host-based IDS that allowed the individual IDS to determine the trust of others using a forgetting factor based on their own experience. Also identity verification and collaboration incentives were provided in the framework between them. Then, Fung et al. in a next work [65] using a Dirichlet model, developed their method to measure the confidence between IDS nodes according to their mutual experience. The experimental results showed that the new method had the ability to increase robustness and efficacy. As positive points, we note the increase of robustness and scalability against common internal menaces. Later, with an objective to minimize costs and false alarms, Fung et al. [66] used a Bayesian approach to feedback approach. They summarized their approach and their framework in 2013 [64] in this final work, they adopted a Bayesian learning approach to assess the performance of each IDS in detecting intrusions.

c. Support Vector Machine (SVM)

Support vector machines are prominent classification techniques applied in many fields like image processing, text classification…etc [149]. The SVM classifier becomes important after the publication of work introduced by Boser et al. [22]. Authors in [22] defined an SVM like a discriminative classifier formally defined by separating hyper planes. SVM is applied in several fields because it relies on solid mathematical evidence [149, 77].

According to Bystritsky et al. [31], SVM is a machine learning method that is widely applied in the field of pattern recognition and intrusion detection.

Fundamental SVM is concerned with two-class issues in the context of the hyper planes defined by several support vectors in which the data is separated [39]. A noteworthy feature of SVM is that its learning ability can be independent of the dimensionality of the feature space [39]. The simplest SVM model is presented in Figure 7 which called the maximum margin classifier [39]. Supervised classification techniques are applied for intrusion detection starting from the Denning's inception model [155].

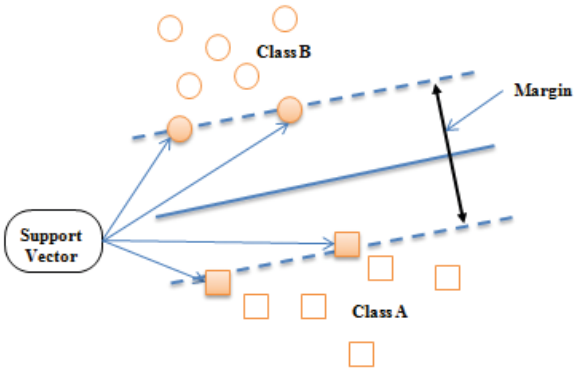


Figure 7. Illustration of the simplest SVM model

Wankhade and Chandrasekaran [188] proposed a system by using an hybrid method. It is a combination of Support Vector Machine (SVM) and Ant Colony Optimization (ACO). Basically, the system collects data across the network and the hybrid method classifies the network activities as normal or abnormal. Also, it can detect unseen attacks with high detection rate with minimal misclassification. Experimental results show that the usage of hybrid method on the CIDS model is better to that of SVM alone, or terms ACO alone, both in of run-time efficiency and detection rate.

Another important work of Teng et al. [177] allowed to develop a self-adaptive and collaborative intrusion detection based on DTs and SVMs.Their model was built and implemented using the Environments-classes, agents, roles, groups, and objects (E-CARGO) model. They also developed adaptive scheduling mechanisms. Experimen-

tal results prove the feasibility and efficiency of the proposed collaborative and adaptive intrusion detection method, tested on KDD cup 1999 data-set.

d. Decision Trees (DT)

Decision tree is one of the most popular classification methods in data mining applications [147]. They are also easy to use and understand. They are made of decision nodes and leaf nodes [147]. After a decision tree is built, the test data from the root node of the DT can be organized with the same structure as the training data [172]. The test is performed with the same test attribute that the root node denotes and, next, the decision procedures take the branch which condition is satisfied of the tested attribute value [172]. The same procedure is done recursively until a leaf node is reached, and a class is assigned to the test cases. DT have been successfully used for intrusion detection tasks since DT can learn a model based on training data and predict whether future data consists of an attack or whether normal data is safe[142].

The advantages of DT are as follow [142]:

– High performance, that allows real time detection, since they allow the creation of an easily interpretable model;

– DT allow to build an easily interpretable models, which is useful for inspection and modification;

– The DT generalization accuracy allows identifying new intrusions.

Also the work of Teng et al. [177] that detailed above, which is a self-adaptive and collaborative intrusion detection based on DTs and SVMs. Results prove that the optimized collaborative and adaptive intrusion detection model based on 2-class SVMs and DTs is more accurate and efficient than the detector system with a set of single type SVMs. The work of Eesa et al. [50] that suggest a novel CIDS based on the combination of Cuttlefish Optimization Algorithm (CFA) and Decision Tree (DT).

e. Deep Learning (DL)

In 2006, Hinton was the first who introduced Deep learning (DL) [84]. DL is the newest advanced in machine learning and has been used in recent research in several fields [18]. A deep learning architecture is structured in a hierarchy, comprised of many levels of features that are designed automatically from higher (input) to lower (output) level [84, 176], as illustrated in Figure 8. In addition, layer generalization involves an algorithm which enables the acquisition of complex data without a manual generalization of human - crafted characteristics [19, 173].

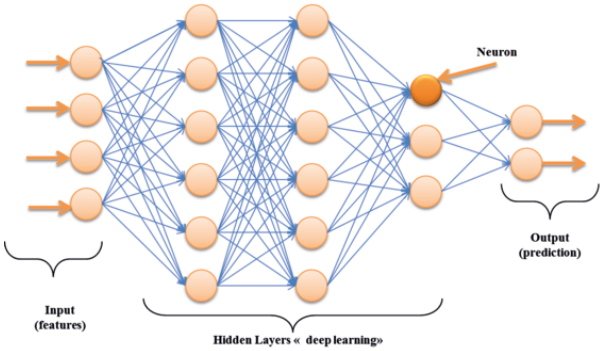


Figure 8. Structure of a deep neural network

After deep learning was introduced, many researchers indicated that deep learning is successful in different fields, such as speech recognition [144], image recognition [35], and even molecular analysis that may lead to the discovery of new drugs [69]. Additionally, it was also used to detect network intrusions and in many other security relating topics [164, 168, 67, 8]. A deep learning algorithm can then be trained as a supervised, unsupervised, and semi-supervised way of learning [3, 103, 120, 118, 199]. As the amount of data and range of applications for machine learning methods continues to grow, the capability to automatically learn the powerful features will grow [18]. Deep learning techniques can be classified into one of three classes, depending on how these techniques can be used [108]:

– Deep networks for unsupervised learning

– Deep networks for supervised learning

– Hybrid deep networks

There is a wide variety of deep learning algorithms that have been employed in intrusion detection [108, 97, 57], such as:

– Restricted Boltzmann machine (RMB);

– Deep Boltzmann machine (DMB);

– Deep belief network (DBN);

– Deep neural network (DNN);

– Generalized denoising Auto-Encoded;

– Recurrent neural network (RNN).

As mentioned previously, deep learning technology was successfully used to build IDS by many authors in recent years. Authors in [68] have used DBN as a classifier for intrusion detection. They have demonstrated that DBN can be used successfully as an efficient IDS. Results show that the DBN model performs better than that of SVM and ANN. Alom et al. [9] also used DBN to detect intrusions. Similarly, Shone et al.[164] presented a novel DL model for intrusion detection.

Marir et al. [125] proposed a distributed deep belief network (DBN) approach for collaborative detection of abnormal behavior in large-scale networks. The developed model discovers the abnormal behavior from large-scale network traffic data using a combination of a deep feature extraction and multi-layer ensemble SVM in a collaborative way. This latter is accomplished in an iterative reduction paradigm based on Spark (a general distributed in-memory computing framework developed at AMP Lab, UC Berkeley). The main purpose of this work is to discover abnormal activity in a large scale network, based on Apache Spark. Results demonstrate the efficiency of the proposed method and its high performances in the detection of abnormal behavior. Four data-sets were used, namely: KDD cup99, NSL-KDD, UNSW-NB15, and CICIDS2017. We note that this work is not based on multi-agent systems.

An other important work of Laqtib et al. [109], considered the hierarchical collaborative IDS using deep learning techniques under MANETs, in which each node has an IDS agent running. The authors presented well-known deep learning models namely: CNN, Inception-CNN, Bi-LSTM, and GRU. Next, they made a systematic comparison of CNN and RNN on the DL-based IDS. Experimental results indicated good performance for all 4 models. But on the Recall, basic CNN and inception-CNN failed, also the Bi-LSTM model obtained worse results on accuracy rates than the other models.

4.3.3 Heuristics

Heuristics signifies "to find", "to know", "to guide an investigation" or "to discover" [110]. Heuristic techniques help to find the best or the closest optimum solutions at an inexpensive computing cost without guarantee of feasibility or optimality [158]. Most of those algorithms have stochastic behavior and imitate biological or physical methods, also completely different categories were considered to categorize meta-heuristic techniques so far [14].

Primitively, the heuristics developed in computer science were depending on the instance problems [170]. Later, advanced studies have proposed robust and general methods, this latter, might be valid to resolving many alternative issues [170].

Greedy or Glutton algorithm is the most used heuristic method that achieves a particularly good performance in the experimental results [200]. Also, it can be much faster than traditional dynamic programming approaches, which produce theoretically optimal solutions [110]. Historically, it was generalized and widely studied by computer scientists in the mid-1980s [129, 132, 182, 194].

The greedy approach involves a factor with littler parameters than the original problem of finding an almost optimal boot configuration, therefore expecting it to be a simpler problem [184]. The intuitive assumption is that one can find the optimal (relative to the likelihood) (k + 1) mixture gotten by local search if one starts local search from the resulting mixture by optimally inserting a new component into the component k optimal mix [184]. The greedy algorithms locally make optimal selections that ultimately extend a global optimum [117]. However, a very important advantage compared to other solutions is that the execution of the calculation costs is low [117]. The use of the Greedy algorithm for intrusion detection is more advantageous, and practical than traditional algorithms [196].

In the work of Fung et al.[64], which has been already detailed in "Machine learning" subsection, the greedy approach was employed in order to determine the smallest number of best acquaintances and to reduce the cost of false alarms.

4.3.4 Meta-heuristics

The expression meta-heuristic may be partially in “meta” and “heuristic” which comes from Greek, “meta” is “higher level” [110]. In addition, meta-heuristics are a collection of intelligent approaches to extend the efficiency of heuristic techniques [158]. A meta-heuristic as denoted in [187] is “an iterative master procedure that guides and modifies the operations of subordinate heuristics to with efficiency turn out high quality solutions". The meta-heuristic can manipulate complete and incomplete solutions as well as a collection of solutions in every iteration [187]. The subordinate heuristic can be procedures, a simple local search, or simply a construction method [187]. The following are algorithms of meta-heuristic methods: Artificial Immune Systems (AIS) [55], Ant Colony Optimization (ACO) [47], Genetic Algorithms [175], particle Swarm Optimization (PSO) [101, 52], etc. Thus, Genetic Algorithms (GA) are one of the most known meta-heuristics.

According to Bobor [20]: “A Genetic Algorithm is a programming technique that uses biological evolution as a problem solving strategy”. It is based on Darwinian concept of evolution and survival of the fittest to augment a population of candidate solutions to a predefined fitness [113, 124]. The progression stages of a genetic algorithm generally begin with a population of randomly and carefully selected chromosomes, which illustrate the problem and depend on its attributes[113, 146]. According to the latter, chromosomes are encoded in the form of bits, characters or numbers ,and a set of chromosomes is called "population" through an evolutionary stage [113]. In the assessment stage, two main operators simulate the use of cross-breeding and mutation, and finally, the chromosome choice is set to the maximum chromosomes for survival and mixing [113, 146]. The efficiency of the algorithms is related to three main factors [150]: fitness functions selection, individuals illustration, and GA parameters.

The effort of mixed GA and intrusion detection can be referred back to 1995, when computer scientists, Crosbie and Spafford applied the agent technology and genetic programming to detect intrusions [42]. Genetic algorithms are used to determine optimal parameters that can be used in other techniques to optimize results and increase IDS accuracy [20, 37], and generally the results of using GA with IDS more effectively [150, 135].

The paper of Janakiraman [91] presents an intelligent learning approach using Genetic Algorithm for Collaborative Intrusion Detection System. The proposed approach uses simple exemplification of rules and fitness function. GA is used to increase the detection rate and reduce the false alarm rate. The selection operation has two processes, namely: calculating the fitness value and sorting it ascendant order. In addition, they generate rules with an effective fitness function which can be used for distributed attacks. In addition, the generated rules can be used with an adaptive cost.

The work of Bukhtoyarov and Zhukov [28] presents a CIDS that uses ensembles of neural networks, which are combined using genetic programming (GP). The experimental results demonstrate that the proposed GP-based systems offers high performances.

In Table 2, we summarize the previously discussed papers, according to the provided taxonomy. Moreover, we highlight the main characteristics of each work, as well as their performance with regard to accuracy, detection rate, and false alarms rate, for those who provided such information.

5 Discussion, open issues, and recommendations

Collaborative intrusion detection systems are very important for network protection. The subject has attracted the interest of many researchers. This is why a wide range of studies and approaches are being implemented with different techniques for the purposes of reaching a high detection accuracy with a very low false alarms rate while ensuring more efficiency and scalability.

In this work, we introduced a three fold classification for collaborative intrusion detection systems (CIDSs). Firstly, according to the system architecture, secondly, according to the used agents category, and finally according to the decision technique implemented within the CIDS. These three classes are discussed and exemplified with the most notable researches that were sufficiently analyzed.

By reviewing nearly two hundred papers, we presented CIDSs, in the architecture classification part, as systems with or without a central component. Based on this first classification, we can note that decentralized and hierarchical CIDS are more scalable than centralized ones, but they are still in the early stages of development. However, and in order to guarantee scalability and performance of CIDS in the decentralized architectures, a particular attention should be paid to information sharing mechanisms.

Using multi-agents technology allows CIDSs to be more efficient, and provide a better detection accuracy. Generally, using MAS makes collaborative detection possible through cooperation and data correlation. The works presented in table **??** show that researchers are still relaying on MAS in collaborative IDS [4, 50, 115, 154], and the obtained results confirm that the distribution and the use of MAS technology play an important role in enhancing the detection accuracy and make systems more effective.

Recently, the number of papers proposing knowledge-based CIDS continuously decreases, mainly because of their orthodox and traditional schemes. Such a fact can be observed in those having proposed expert system-based [169] and ontology-based CIDS [1, 26]. Therefore, computer security researchers oriented their efforts towards machine-learning, heuristics and meta-heuristics based paradigms.

Heuristics and meta-heuristics methods are still implemented in several works, which are generally based on greedy algorithm: [64], and genetic algorithms [28, 91]. Also, the combination of heuristic and meta-heuristic methods and machine learning techniques was considered, such as in [28]. Such approaches allowed security systems to be more accurate and more efficient.

Machine learning techniques are still extensively used in many recent work, and that given the great potential of these techniques to address the problems inherent in IDS and CIDS. The most used ML techniques are: Neural Networks [28, 165, 166], Bayesian Networks [152, 64], SVM [177, 188], Decision Trees [50, 177], and Deep Learning [109].

In the last five years, deep learning techniques have been successfully used to propose more efficient IDSs with very high detection accuracy [9, 68, 164]. However, and according to the current state of the art, we found only few proposed approaches for DL-based CIDS [125], and the work of [109] have combined DL technique and MAS-based CIDS. We would like to point that designing a DL-based CIDSs require very large and diverse datasets in to train a highly accurate detection model.

One of the main limitations of the current CIDS-related research is the lack of commonly used benchmark testing that allows the comparison of the different solutions in a common environment. Moreover, it requires extra research efforts to acquire datasets that can allow an equitable evaluation of these solutions. Indeed, it is extremely hard to analyze and compare the results of the proposed solutions, when no common dataset is used. We also noticed that some solutions used old datasets such KDD and KDD-NSL, which we believe do not reflect the current threats. It is also very hard to identify the most appropriate dataset for a fair evaluation of the proposed CIDS solutions. We note that, choosing the right dataset [153], as well as optimizing the performances of CIDS, and improving realtime capabilities remain, so far, significant open problems.

Finally, we can note that the collaborative intrusion detection is a vast field; where researchers are still proposing novel methods that combine different techniques, and technologies in order to develop a highly accurate defense systems that are able to detect efficiently and in realtime new attacks with fewer false alarms.

Table 2. A list of well cited papers summarized in the survey
AC: Accuracy (%), DR: Detection Rate (%), FA: False alarms (%)

Work	Year	Architecture	Agent type	Technique	Features	Results
[169]	1991	Centralized	N/A	Expert system	Non scalable; Single point of failure; Reducing the attack traffic for a given network; Viability of distributed architecture in solving the network-user identification problem; Real traffic;	N/A
[171]	2000	Hierarchical	Autonomous agent	N/A	No single point of failure; Limited scalability; Good performance; Real traffic;	N/A
[98]	2005	Decentralized	Mobile and Static agent	N/A	High and better scalability; No single point of failure; High performance; Real traffic;	N/A
[152]	2006	Decentralized	N/A	Bayesian Networks	Good performances; Real traffic;	AC:90% DR:94.54% FA:N/A
[1]	2009	Decentralized	N/A	Ontology	Reduce the rate of false alarms; Reduction in cost; KDD cup 99 data-set;	AC:0.015% DR:99.9% FA:2.5%
[91]	2009	Decentralized	N/A	Genetic algorithm	effective and adaptive cost of detection; DARPA data-set;	N/A
[165]	2011	Decentralized	N/A	Neural Networks	minimize generating false alarms; Good detection rate; real traffic;	N/A
[136]	2012	Decentralized	N/A	N/A	High and better scalability; No single point of failure; High performance; KDD cup 99 data-set;	AC:80% DR:N/A FA:N/A
[64]	2013	Decentralized	N/A	Bayesian Networks and Greedy Algorithm	Good performances; reduces the cost of risks from false decisions; incentive-compatible; scalable; robust; Real traffic;	N/A
[26]	2014	Decentralizes	N/A	Ontology	Reduce the overload of the use of its multiple components; KDD cup 99 data-set;	AC:99.74% DR:N/A FA:N/A

Work	Year	Architecture	Agent type	Technique	Features	Results
[28]	2014	Decentralized	N/A	Genetic Programming, Neural Networks	High efficiency; KDD cup 99 data-set;	AC:N/A DR:97.2% FA:0.3%
[5]	2014	Decentralized	Autonomous and Mobile agents	Artificial Immune System	High and better scalability; No single point of failure; High performance; NSL and KDD cup 99 data-set;	N/A
[133]	2014	Decentralized	Situated agent	N/A	Good detection rate of DDoS attack; Scalable; minimized false positives alarms; Real traffic;	AC:N/A DR:95% FA:N/A
[166]	2014	Decentralized	N/A	Neural Networks	good detection accuracy; efficiency system; reduce the workload; KDD cup 99 data-set;	N/A
[100]	2015	Decentralized	Mobile agent	N/A	High and better scalability; No single point of failure; High performance; Real traffic;	N/A
[6]	2015	Hierarchical	Reactive agent	Case-Based Reasoning (CBR)	No single point of failure;Limited scalability; Good performance;	N/A
[188]	2016	Decentralized	N/A	SVM – ACO	a higher detection rate; faster running time which; system is very efficient; KDD cup 99 data-set; poor performance of SVM and high computation;	AC:N/A DR:84.19% FA:N/A
[177]	2017	Decentralized	N/A	Decision tree and SVM	good detection accuracy and efficiency; KDD cup 99 data-set; poor performance of SVM and high computation;	AC:89.02% DR:N/A FA:12.19%
[50]	2017	Decentralized	Mobile agent	Decision Tree	Good performance when using 5 features; U2R attack give better performance with 41 features; KDD cup 99 data-set;	AC:N/A DR:99.4% FA:N/A

Work	Year	Architecture	Agent type	Technique	Features	Results
[115]	2018	Hierarchical	Mobile agent	N/A	No single point of failure;Limited scalability; Good performance; Solve the problem of bottleneck; KDD cup 99 data-set;	N/A
[4]	2018	Decentralized	Mobile agent and reactive agent	N/A	High and better scalability; No single point of failure; High performance; effective system; Real traffic; adaptive system; reduce the workload; detect known and unknown attacks;	AC:N/A DR:81% FA:11%
[154]	2019	Decentralized	Mobile agent	N/A	High and better scalability; No single point of failure; High performance; effective system; Real traffic;	N/A
[109]	2019	Hierarchical	N/A	Deep Learning	Good performance for the 4 model; Bi-LSTM model was the worst in AC; NSL-KDD data-set	AC:89.03% DR:97.78% FA:N/A
[121]	2019	Decentralized	N/A	Data Mining	Effective system; High response time; Good performance; Real traffic;	AC:92.76% DR:N/A FA:N/A

Therefore, our recommendations in order to build more efficient CIDS can be summarized in the following points:

- CIDS should be oriented towards the Cloud computing environment, especially for centralized and hybrid architectures, which will offer more flexibility and higher performances.
- The evaluation of each CIDS should be performed in a heterogeneous network environment and using a large amount of real network traffic data or at least recently published datasets;
- The implementation of a secure connection at MAS level between agents should be considered;
- Providing protection mechanisms for agents against adversarial attacks;
- Machine learning techniques have been able to provide very good performances in the field of intrusion detection. Therefore, we believe that future CIDS approaches should increase the application of machine learning techniques, and especially Deep Learning, and that in order to overcome the previously discussed challenges.

6 Conclusion

The collaboration among a geographically distant IDS has led to the emergence of the so called CIDS. The latter rely on the correlation of security events in order to ensure better protection against the recent threats. MAS have been successfully used in this context since they intuitively provide the required cooperation and collaboration mechanisms. In this review, we have proposed a full taxonomy of MAS-based collaborative intrusion detection systems, in which we suggested a categorization based on several criteria such as the adopted CIDS' architecture, the used agents technology, and the used decision techniques. Based on this survey, we can conclude that CIDS have the potential to provide a good level of protection, provide a real-time response, and can be deployed in large-scale networks. However, we have identified some limitations, which are related to the lack of commonly used benchmark testing, since the proposed studies used different datasets to evaluate their performances, and only very few of them have been deployed in real large-scale networks. In addition, most of the existing solutions rely on old datasets, and detection techniques, which we believe are not adequate with regard of the nature of the current threats.

Finally, we believe that the future efforts for designing efficient CIDS should be oriented towards cloud-based architectures, and employ cutting edge technologies such deep learning, and blockchain.

References

[1] F. Abdoli and M. Kahani. Ontology-based distributed intrusion detection system. In 2009 14th International CSI Computer Conference, pages 65–70. IEEE, oct 2009.

[2] Yuehui. ABRAHAM, Ajith; GROSAN, Crina; et CHEN. Cyber security and the evolution in intrusion detection systems. Journal of Engineering and Technology, pages 0973–2632, 2005.

[3] Abdulla Amin Aburomman and Mamun Bin Ibne Reaz. Survey of learning methods in intrusion detection systems. In 2016 International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES), pages 362–365. IEEE, nov 2016.

[4] Omar Achbarou, My Ahmed El Kiram, Outmane Bourkoukou, and Salim Elbouanani. A New Distributed Intrusion Detection System Based on Multi-Agent System for Cloud Environment. International Journal of Communication Networks and Information Security (IJCNIS), 10(3):2018, 2018.

[5] Neda Afzali Seresht and Reza Azmi. MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach. Engineering Applications of Artificial Intelligence, 35:286–298, oct 2014.

[6] Mohssine El Ajjouri, Siham Benhadou, and Hicham Medromi. New collaborative intrusion detection architecture based on multi agent systems. In 2015 International Conference on Wireless Networks and Mobile Communications (WINCOM), pages 1–6. IEEE, oct 2015.

[7] A. Sima. AKYAZI, Ugur et UYAR. Distributed detection of DDoS attacks during the intermediate phase through mobile agents. Computing and Informatics, 31(4):759—-778, 2012.

[8] Arwa Aldweesh, Abdelouahid Derhab, and Ahmed Z Emam. Deep learning approaches for

anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189:105124, 2020.

[9] Md. Zahangir Alom, VenkataRamesh Bontupalli, and Tarek M. Taha. Intrusion detection using deep belief networks. In 2015 National Aerospace and Electronics Conference (NAECON), pages 339–344. IEEE, jun 2015.

[10] Dinesha Hagare Annappaian and Vinod Kumar Agrawal. Cloud Services Usage Profile Based Intruder Detection and Prevention System: Intrusion Meter. Transactions on Networks and Communications, 2(6):12–24, dec 2014.

[11] A.F. Atiya, S.M. El-Shoura, S.I. Shaheen, and M.S. El-Sherif. A comparison between neural-network forecasting techniques-case study: river flow forecasting. IEEE Transactions on Neural Networks, 10(2):402–409, mar 1999.

[12] A.B. Badiru. Computational survey of univariate and multivariate learning curve models. IEEE Transactions on Engineering Management, 39(2):176–188, may 1992.

[13] Daniel Barbara, Ningning Wu, and Sushil Jajodia. Detecting novel network intrusions using bayes estimators. In Proceedings of the 2001 SIAM International Conference on Data Mining, pages 1–17. SIAM, 2001.

[14] Zahra Beheshti and Siti Mariyam Hj Shamsuddin. A review of population-based meta-heuristic algorithms. Int. J. Adv. Soft Comput. Appl, 5(1):1–35, 2013.

[15] Mohamed Belaoued, Abdelaziz Boukellal, Mohamed Amir Koalal, Abdelouahid Derhab, Smaine Mazouzi, and Farrukh Aslam Khan. Combined dynamic multi-feature and rule-based behavior for accurate malware detection. International Journal of Distributed Sensor Networks, 15(11):155014771988990, nov 2019.

[16] Mohamed Belaoued, Abdelouahid Derhab, Smaine Mazouzi, and Farrukh Aslam Khan. MACoMal: A Multi-Agent Based Collaborative Mechanism for Anti-Malware Assistance. IEEE Access, 8:14329–14343, 2020.

[17] Mohamed Belaoued, Bouchra Guelib, Yasmine Bounaas, Abdelouahid Derhab, and Mahmoud Boufaida. Malware detection system based on an in-depth analysis of the portable executable headers. In International conference on machine learning for networking, pages 166–180. Springer, 2018.

[18] Y. Bengio. Learning Deep Architectures for AI. Foundations and Trends® in Machine Learning, 2(1):1–127, 2009.

[19] Y. Bengio, A. Courville, and P. Vincent. Representation Learning: A Review and New Perspectives. IEEE Transactions on Pattern Analysis and Machine Intelligence, 35(8):1798–1828, aug 2013.

[20] Vladimir Bobor. Efficient Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms. Department of Computer and Systems Sciences, Stockholm University/Royal Institute of Technology, KTH/DSV, 2006.

[21] Sven-Erik Bornscheuer. Integrating reactive and reflective reasoning by generating rational models. pages 83–94. 1998.

[22] Bernhard E. Boser, Isabelle M. Guyon, and Vladimir N. Vapnik. A training algorithm for optimal margin classifiers. In Proceedings of the fifth annual workshop on Computational learning theory - COLT '92, pages 144–152, New York, New York, USA, 1992. ACM Press.

[23] K. Boudaoud, H. Labiod, R. Boutaba, and Z. Guessoum. Network security management with intelligent agents. In IEEE Symposium Record on Network Operations and Management Symposium, pages 579–592. IEEE, 2000.

[24] Imen Brahmi and Hanen Brahmi. OMAIDS: A Multi-agents Intrusion Detection System Based Ontology. pages 156–163. 2015.

[25] Imen Brahmi, Sadok Ben Yahia, Hamed Aouadi, and Pascal Poncelet. Towards a multiagent-based distributed intrusion detection system using data mining approaches. In International Workshop on Agents and Data Mining Interaction, pages 173–194. Springer, 2011.

[26] Krupa Brahmkstri, Devasia Thomas, S. T. Sawant, Avdhoot Jadhav, and D. D. Kshirsagar. Ontology Based Multi-Agent Intrusion Detection System for Web Service Attacks Using Self Learning. pages 265–274. 2014.

[27] D Brickley and R V Guha. Rdfs: Resource description framework schema. W3C Working Draft, 12, 2002.

[28] Vladimir Bukhtoyarov and Vadim Zhukov. Ensemble-Distributed Approach in Classification Problem Solution for Intrusion Detection Systems. pages 255–265. 2014.

[29] Dusan Bulatovic and Dusan Velasevic. A Distributed Intrusion Detection System Based on Bayesian Alarm Networks. pages 219–228. 1999.

[30] Dusan Bulatovic and Dusan Velasevic. A distributed intrusion detection system based on bayesian alarm networks. In International Exhibition and Congress on Network Security, pages 219–228. Springer, 1999.

[31] Alexander Bystritsky, Deborah L. Ackerman, Richard M. Rosen, Tanya Vapnik, Eda Gorbis, Karron M. Maidment, and Sanjaya Saxena. Augmentation of Serotonin Reuptake Inhibitors in Refractory Obsessive-Compulsive Disorder Using Adjunctive Olanzapine. The Journal of Clinical Psychiatry, 65(4):565–568, apr 2004.

[32] James Cannady, Jay Harrell, et al. A comparative analysis of current intrusion detection technologies. In Proceedings of the Fourth Technology for Information Security Conference, volume 96, 1996.

[33] James D. Cannady. Artificial neural networks for misuse detection. In Proceedings of the 21st National information systems security conference, volume 26, pages 368–381. Baltimore, 1998.

[34] Brian Caswell and Jay Beale. Snort 2.1 intrusion detection. Elsevier, 2004.

[35] Tsung Han Chan, Kui Jia, Shenghua Gao, Jiwen Lu, Zinan Zeng, and Yi Ma. PCANet: A Simple Deep Learning Baseline for Image Classification? IEEE Transactions on Image Processing, 24(12):5017–5032, 2015.

[36] Jennifer A. CHANDLER. Security in cyberspace: combatting distributed denial of service attacks. U. Ottawa L. & Tech. J., 1, 2003.

[37] RUCHI CHATURVEDI, BABITA PATHIK, and SHIV KUMAR. Intrusion Detection Using Data Mining Along Fuzzy Logic & Genetic Algorithms. Journal of Computer and Information Technology, 09(01):9–13, 2018.

[38] Ping Chen, Lieven Desmet, and Christophe Huygens. A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security, pages 63–72. Springer, 2014.

[39] Wun-Hwa Chen, Sheng-Hsun Hsu, and Hwang-Pin Shen. Application of SVM and ANN for intrusion detection. Computers & Operations Research, 32(10):2617–2634, oct 2005.

[40] T. Chheda, T. Mukerji, A.H. Scheirer, and S.A. Graham. Bayesian Networks for Decisions under Uncertainty in Basin Modeling. jun 2018.

[41] Crispin Cowan, F Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole. Buffer overflows: Attacks and defenses for the vulnerability of the decade. In Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, volume 2, pages 119–129. IEEE, 2000.

[42] Mark Crosbie and Eugene H Spafford. Applying Genetic Programming to Intrusion Detection. Working Notes for the AAAI Symposium on Genetic Programming, pages 1–8, 1995.

[43] Fatemeh Daneshfar and Hassan Bevrani. Multiagent systems in control engineering: a survey. Journal of Control Science and Engineering, 2009, 2009.

[44] Amin Dastanpour, Suhaimi Ibrahim, Reza Mashinchi, and Ali Selamat. Comparison of genetic algorithm optimization on artificial neural network and support vector machine in intrusion detection system. In 2014 IEEE Conference on Open Systems (ICOS), pages 72–77. IEEE, oct 2014.

[45] M. de Boer, Pieter; Pels. Host-based Intrusion Detection Systems. Retrieved from. 2005.

[46] Dorothy Denning and Peter G Neumann. Requirements and model for IDES-a real-time intrusion-detection expert system, volume 8. SRI International, 1985.

[47] Marco Dorigo, Vittorio Maniezzo, and Alberto Colorni. Ant system: Optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 26(1):29–41, 1996.

[48] Ali Dorri, Salil S Kanhere, and Raja Jurdak. Multiagent systems: A survey. IEEE Access, 6:28573–28593, 2018.

[49] Wesley M Eddy. Defenses against tcp syn flooding attacks. The Internet Protocol Journal, 9(4):2–16, 2006.

[50] Adel S. Eesa, Adnan M. Abdulazeez, and Zeynep Orman. A DIDS Based on The Combination of Cuttlefish Algorithm and Decision Tree. Science Journal of University of Zakho, 5(4):313, dec 2017.

[51] Mohamad. EID. A new mobile agent-based intrusion detection system using distributed sensors. proceeding of FEASC, 2004.

[52] Mohamed El Bekri and Ouafaa Diouri. Pso based intrusion detection: A pre-implementation discussion. Procedia Computer Science, 160:837–842, 2019.

[53] Charles Elkan. Results of the KDD'99 classifier learning. ACM SIGKDD Explorations Newsletter, 1(2):63, jan 2000.

[54] W. Fan, M. Miller, S. Stolfo, W. Lee, and P. Chan. Using artificial anomalies to detect unknown and known network intrusions. Knowledge and Information Systems, 6(5):507–527, sep 2004.

[55] J. Doyne Farmer, Norman H. Packard, and Alan S. Perelson. The immune system, adaptation, and machine learning. Physica D: Nonlinear Phenomena, 22(1-3):187–204, 1986.

[56] Jacques Ferber and Gerhard Weiss. Multi-agent systems: an introduction to distributed artificial intelligence, volume 1. Addison-Wesley Reading, 1999.

[57] Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, and Helge Janicke. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50:102419, 2020.

[58] E.A. Fisch, G.B. White, and U.W. Pooch. The design of an audit trail analysis tool. In Tenth Annual Computer Security Applications Conference, pages 126–132. IEEE Comput. Soc. Press, 1994.

[59] Gianluigi Folino and Pietro Sabatino. Ensemble based collaborative and distributed intrusion detection systems: A survey. Journal of Network and Computer Applications, 66:1–16, 2016.

[60] Gianluigi Folino and Pietro Sabatino. Ensemble based collaborative and distributed intrusion detection systems: A survey. Journal of Network and Computer Applications, 66:1–16, may 2016.

[61] Kevin L Fox, Ronda R Henning, Jonathan H Reed, and Richard P Simonian. A neural network approach towards intrusion detection. Proceedings of the 13th National Computer Security Conference, 1:125–134, 1990.

[62] Stefan Fünfrocken. Transparent migration of java-based mobile agents: Capturing and re-establishing the state of java programs. Personal and Ubiquitous Computing, 2(2):109–116, jun 1998.

[63] Carol J Fung, Olga Baysal, Jie Zhang, Issam Aib, and Raouf Boutaba. Trust management for host-based collaborative intrusion detection. In International Workshop on Distributed Systems: Operations and Management, pages 109–122. Springer, 2008.

[64] Carol J Fung and Raouf Boutaba. Design and management of collaborative intrusion detection networks. In 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), pages 955–961. IEEE, 2013.

[65] Carol J Fung, Jie Zhang, Issam Aib, and Raouf Boutaba. Robust and scalable trust management for collaborative intrusion detection. In 2009 IFIP/IEEE International Symposium on Integrated Network Management, pages 33–40. IEEE, 2009.

[66] Carol J Fung, Quanyan Zhu, Raouf Boutaba, and Tamer Başar. Bayesian decision aggregation in collaborative intrusion detection networks. In 2010 IEEE Network Operations and Management Symposium-NOMS 2010, pages 349–356. IEEE, 2010.

[67] Sunanda Gamage and Jagath Samarabandu. Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications, page 102767, 2020.

[68] Ni Gao, Ling Gao, Quanli Gao, and Hai Wang. An Intrusion Detection Model Based on Deep Belief Networks. In 2014 Second International Conference on Advanced Cloud and Big Data, pages 247–252. IEEE, nov 2014.

[69] Erik Gawehn, Jan A. Hiss, and Gisbert Schneider. Deep Learning in Drug Discovery. Molecular Informatics, 35(1):3–14, 2016.

[70] Michael R Genesereth and Nils J Nilsson. Logical foundations of artificial. Intelligence. Morgan Kaufmann, 2, 1987.

[71] Anup K Ghosh, James Wanken, and Frank Charron. Detecting anomalous and unknown intrusions against programs. In Proceedings 14th annual computer security applications conference (Cat. No. 98Ex217), pages 259–267. IEEE, 1998.

[72] Rajeev Gopalakrishna and E.H. Spafford. A framework for distributed intrusion detection using interest driven cooperating agents. Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001), pages 1–23, 2001.

[73] Shaw Green, L. Hurst, B. Nangle, and P. Cunningham. Software agents: A review. Technical Report, 66(May):26–39, 1997.

[74] Sander Greenland, Judea Pearl, James M Robins, and Others. Causal diagrams for epidemiologic research. Epidemiology, 10:37–48, 1999.

[75] Thomas R. Gruber. A translation approach to portable ontology specifications. Knowledge Acquisition, 5(2):199–220, jun 1993.

[76] Thomas R. Gruber. Toward principles for the design of ontologies used for knowledge sharing? International Journal of Human-Computer Studies, 43(5-6):907–928, nov 1995.

[77] Jie Gu, Lihong Wang, Huiwen Wang, and Shanshan Wang. A novel approach to intrusion detection using svm ensemble with feature augmentation. Computers & Security, 86:53–62, 2019.

[78] Yunchuan Guo, Han Zhang, Lingcui Zhang, Liang Fang, and Fenghua Li. A game theoretic approach to cooperative intrusion detection. Journal of computational science, 30:118–126, 2019.

[79] Megha Gupta. Hybrid Intrusion Detection System: Technology and Development. International Journal of Computer Applications, 115(9):5–8, apr 2015.

[80] D. Hammerstrom. Working with neural networks. IEEE Spectrum, 30(7):46–53, jul 1993.

[81] Khadijah M Hanga and Yevgeniya Kovalchuk. Machine learning and multi-agent systems in oil and gas industry applications: A survey. Computer Science Review, 34:100191, 2019.

[82] David Heckerman. A tutorial on learning with bayesian networks. Microsoft Research. 1995.

[83] Álvaro Herrero and Emilio Corchado. Multiagent systems for network intrusion detection: A review. In Computational Intelligence in Security for Information Systems, pages 143–154. Springer, 2009.

[84] Geoffrey E. Hinton, Simon Osindero, and Yee-Whye Teh. A Fast Learning Algorithm for Deep Belief Nets. Neural Computation, 18(7):1527–1554, jul 2006.

[85] Neminath Hubballi and Nikhil Tripathi. An event based technique for detecting spoofed ip packets. Journal of Information Security and Applications, 35:32–43, 2017.

[86] Ezzureen Faznien Ibrahim and Shahrinaz Ismail. Detection ddos using ids in cloud computing. Journal of Computing Technologies and Creative Content (JTec), 3(1):4–6, 2019.

[87] Mohamed Idhammad, Karim Afdel, and Mustapha Belouch. Distributed intrusion detection system for cloud environments based on data mining techniques. Procedia Computer Science, 127:35–41, 2018.

[88] James P. Ignizio. A brief introduction to expert systems. Computers & Operations Research, 17(6):523–533, jan 1990.

[89] Neil C Ingram, Dennis J ; Kremer, H S ; Rowe. Distributed Intrusion Detection for Computer Systems Using Communicating Agents. MARINE CORPS WARFIGHTING LAB QUANTICO VA, 2000.

[90] Kuldeep Jachak and Ashish Barua. Distributed intrusion detection using mobile agent in distributed system. IJCA Proceedings on Emerging Trends in Computer Science and Information Technology (ETCSIT2012), 3:1–6, 2012.

[91] S Janakiraman. An Intelligent Distributed Intrusion Detection System using Genetic Algorithm. Journal of Convergence Information Technology, 4(1):70–76, 2009.

[92] Wayne Jansen, Peter Mell, Tom Karygiannis, and Don Marks. Applying Mobile Agents to Intrusion Detection and Response. NIST Interim Report (IR) - 6416, (October):1–46, 1999.

[93] Nicholas R Jennings and Michael Wooldridge. Applications of intelligent agents. In Agent technology, pages 3–28. Springer, 1998.

[94] Dongzi Jin, Yiqin Lu, Jiancheng Qin, Zhe Cheng, and Zhongshu Mao. Swiftids: Real-time intrusion detection system based on lightgbm and parallel intrusion detection mechanism. Computers & Security, 97:101984, 2020.

[95] Ak Jones and Rs Sielken. Computer system intrusion detection: A survey. Computer Science Technical Report, pages 1–25, 2000.

[96] Youna Jung, Minsoo Kim, Amirreza Masoumzadeh, and James BD Joshi. A survey of security issue in multi-agent systems. Artificial Intelligence Review, 37(3):239–260, 2012.

[97] C Kalimuthan and J Arokia Renjit. Review on intrusion detection using feature selection with machine learning techniques. Materials Today: Proceedings, 2020.

[98] Pradeep Kannadiga and Mohammad Zulkernine. DIDMA: A distributed intrusion detection system using mobile agents. In Proceedings - Sixth Int. Conf. on Softw. Eng., Artificial Intelligence, Netw. and Parallel/Distributed Computing and First ACIS Int. Workshop on Self-Assembling Wireless Netw., SNPD/SAWN 2005, volume 2005, pages 238–245. IEEE, 2005.

[99] Shafiullah Khan, Kok Keong Loo, and Zia Ud Din. Framework for intrusion detection in IEEE 802.11 wireless mesh networks. International Arab Journal of Information Technology, 7(4):435–440, 2010.

[100] Supriya Khobragade and Puja Padiya. Distributed Intrusion Detection System Using Mobile Agent. International Journal of Engineering and Innovative Technology (IJEIT), 5(4), 2015.

[101] Serkan Kiranyaz. Particle swarm optimization. In Adaptation, Learning, and Optimization, volume 15, pages 45–82. Citeseer, 2014.

[102] Sotiris B Kotsiantis, I Zaharakis, and P Pintelas. Supervised machine learning: A review of classification techniques. Emerging artificial intelligence applications in computer engineering, 160:3–24, 2007.

[103] Praful Koturwar, Sheetal Girase, and Debajyoti Mukhopadhyay. A Survey of Classification Techniques in the Area of Big Data. mar 2015.

[104] Tiina Kovanen, Gil David, and Timo Hämäläinen. Survey: Intrusion detection systems in encrypted traffic. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems, pages 281–293. Springer, 2016.

[105] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. Bayesian event classification for intrusion detection. In 19th Annual Computer Security Applications Conference, 2003. Proceedings., pages 14–23. IEEE, 1999.

[106] Christopher Kruegel and Thomas Toth. Distributed Pattern Detection for Instrusion Detection. Ndss, 1, 2002.

[107] Tsuang Kuo, Anil Mital, and Sam Anand. An introduction to expert systems in production and manufacturing engineering: the structure, development process and applications. In Handbook of Expert Systems Applications in Manufacturing Structures and rules, pages 1–20. Springer Netherlands, Dordrecht, 1994.

[108] Donghwoon Kwon, Hyunjoo Kim, Jinoh Kim, Sang C. Suh, Ikkyun Kim, and Kuinam J. Kim. A survey of deep learning-based network anomaly detection. Cluster Computing, 22(S1):949–961, jan 2019.

[109] Safaa Laqtib, Khalid El Yassini, and Moulay Lahcen Hasnaoui. A deep learning methods for intrusion detection systems based machine learning in manet. In Proceedings of the 4th International Conference on Smart City Applications, pages 1–8, 2019.

[110] Alina Lazar. Heuristic Knowledge Discovery for Archaeological Data Using Genetic Algorithms and Rough Sets. Heuristic and Optimization for Knowledge Discovery, pages 263–278, 2011.

[111] S.C. Lee and D.V. Heinbuch. Training a neural-network based intrusion detector to recognize novel attacks. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 31(4):294–299, jul 2001.

[112] Wenke Lee and Salvatore J. Stolfo. A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security, 3(4):227–261, nov 2000.

[113] Wei Li. Using genetic algorithm for network intrusion detection. Proceedings of the United States Department of Energy Cyber Security Group 2004 Training Conference, Kansas City, Kansas, 1:24–27, 2004.

[114] Wenjuan Li and Lam For Kwok. Challenge-based collaborative intrusion detection networks under passive message fingerprint attack: a further analysis. Journal of Information Security and Applications, 47:1–7, 2019.

[115] Yongzhong Li, Miao Du, and Jing Xu. A New Distributed Intrusion Detection Method Based on Immune Mobile Agent. In Proceedings - 2018 6th International Conference on Advanced Cloud and Big Data, CBD 2018, pages 215–219. IEEE, 2018.

[116] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1):16–24, jan 2013.

[117] Martin Andreoni Lopez, Diogo Menezes Ferrazani Mattos, and Otto Carlos M. B. Duarte. An elastic intrusion detection system for software networks. Annals of Telecommunications, 71(11-12):595–605, dec 2016.

[118] Manuel Lopez-Martin, Belen Carro, and Antonio Sanchez-Esguevillas. Application of deep reinforcement learning to intrusion detection for supervised problems. Expert Systems with Applications, 141:112963, 2020.

[119] Gehao Lu and Joan Lu. Background review for neural trust and multi-agent system. In Natural Language Processing: Concepts, Methodologies, Tools, and Applications, pages 1–22. IGI Global, 2020.

[120] Namratha M and Prajwala TR. A Comprehensive Overview of Clustering Algorithms in Pattern Recognition. IOSR Journal of Computer Engineering, 4(6):23–30, 2012.

[121] Jamila Manan, Atiq Ahmed, Ihsan Ullah, Leïla Merghem-Boulahia, and Dominique Gaïti. Distributed intrusion detection scheme for next generation networks. Journal of Network and Computer Applications, 147:102422, 2019.

[122] Frank Manola, Eric Miller, Brian McBride, and Others. RDF primer. W3C recommendation, 10(1-107):6, 2004.

[123] Mirco Marchetti, Fabio Pierazzi, Michele Colajanni, and Alessandro Guido. Analysis of high volumes of network traffic for advanced persistent threat detection. Computer Networks, 109:127–141, 2016.

[124] Adam. MARCZYK. Genetic algorithms and evolutionary programing. Studies in Computational Intelligence, 652:309–348, 2017.

[125] Naila Marir, Huiqiang Wang, Guangsheng Feng, Bingyang Li, and Meijuan Jia. Distributed Abnormal Behavior Detection Approach Based on Deep Belief Network and Ensemble SVM Using Spark. IEEE Access, 6:59657–59671, 2018.

[126] Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, and Raouf Boutaba. Collaborative security: A survey and taxonomy. ACM Computing Surveys (CSUR), 48(1):1–42, 2015.

[127] Negnevitsky Michael. Artificial intelligence a guide to intelligent systems, 2005.

[128] H Sardana Milan and Kamalpreet Singh. Reducing false alarms in intrusion detection systems–a survey. International Research Journal of Engineering and Technology (IRJET) e-ISSN, pages 2395–0056, 2018.

[129] Webb Miller and Eugene W. Myers. A file comparison program. Software: Practice and Experience, 15(11):1025–1040, nov 1985.

[130] Jelena Mirkovic, Gregory Prier, and Peter Reiher. Attacking ddos at the source. In 10th IEEE International Conference on Network Protocols, 2002. Proceedings., pages 312–321. IEEE, 2002.

[131] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan. A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 36(1):42–57, jan 2013.

[132] Eugene W. Myers. AnO(ND) difference algorithm and its variations. Algorithmica, 1(1-4):251–266, nov 1986.

[133] Abdenacer Nafir, Smaine Mazouzi, and Salim Chikhi. Collective intrusion detection in wide area networks. INISTA 2014 - IEEE International Symposium on Innovations in Intelligent Systems and Applications, Proceedings, pages 46–51, 2014.

[134] Maria Nenova, Denis Atanasov, Kiril Kassev, and Andon Nenov. Intrusion detection system model implementation against ddos attacks. In 2019 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS), pages 1–4. IEEE, 2019.

[135] Minh Tuan Nguyen and Kiseon Kim. Genetic convolutional neural network for intrusion detection systems. Future Generation Computer Systems, 113:418–427, 2020.

[136] O Oriola, AB Adeyemo, and ABC Robert. Distributed intrusion detection system using p2p agent mining scheme. African Journal of Computing & ICT, 5(2):3–10, 2012.

[137] Suad Mohammed Othman, Nabeel T Alsohybe, Fadl Mutaher Ba-Alwi, and Ammar Thabit Zahary. Survey on intrusion detection system types. International Journal of Cyber-Security and Digital Forensics, 7(4):444–463, 2018.

[138] Amrit Pal Singh and Manik Deep Singh. Analysis of Host-Based and Network-Based Intrusion Detection System. International Journal of Computer Network and Information Security, 6(8):41–47, jul 2014.

[139] Nicholas Pappas. Network IDS and IPS Deployment Strategies. SANS Institute, 2008.

[140] Animesh Patcha and Jung Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12):3448–3470, aug 2007.

[141] Marek Pawlicki, Michał Choraś, and Rafał Kozik. Defending network intrusion detection systems against adversarial evasion attacks. Future Generation Computer Systems, 2020.

[142] Sandhya Peddabachigari, Ajith Abraham, and Johnson Thomas. Intrusion Detection Systems Using Decision Trees and Support Vector Machines. International Journal of Applied Science and Computations, 11(3):118–134, 2004.

[143] Daniel Pérez, Serafín Alonso, Antonio Morán, Miguel A. Prada, Juan José Fuertes, and Manuel Domínguez. Comparison of Network Intrusion Detection Performance Using Feature Representation. pages 463–475. 2019.

[144] Stavros Petridis, Themos Stafylakis, Pingehuan Ma, Feipeng Cai, Georgios Tzimiropoulos, and Maja Pantic. End-to-End Audiovisual Speech Recognition. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 6548–6552. IEEE, apr 2018.

[145] John Pinkston, Jeffrey Undercoffer, Anupam Joshi, and Timothy Finin. A target-centric ontology for intrusion detection. In In proceeding of the IJCAI-03 Workshop on Ontologies and Distributed Systems. Acapulco, August 9 th. Citeseer, 2004.

[146] Hartmnt Pohlheim. "Genetic and Evolutionary Algorithms: Principles, Methods and Algorithms." Genetic and Evolutionary Algorithm Toolbox. Evolutionäre Algorithmen, 30, 2001.

[147] J Ross Quinlan. Constructing decision tree. C4, 5:17–26, 1993.

[148] Shahid Raza, Linus Wallgren, and Thiemo Voigt. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8):2661–2674, nov 2013.

[149] R. Ravinder Reddy, Y Ramadevi, and K. V. N Sunitha. Effective discriminant function for intrusion detection using SVM. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pages 1148–1153. IEEE, sep 2016.

[150] Ren Hui Gong, M. Zulkernine, and P. Abolmaesumi. A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection. In Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed

Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05), pages 246–253. IEEE.

[151] Hamed Rezaee and Farzaneh Abdollahi. Average consensus over high-order multiagent systems. IEEE Transactions on Automatic Control, 60(11):3047–3052, 2015.

[152] AHM Rezaul Karim, RMAP Rajatheva, and Kazi M Ahmed. An efficient collaborative intrusion detection system for manet using bayesian approach. In Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems, pages 187–190, 2006.

[153] Markus Ring, Sarah Wunderlich, Deniz Scheuring, Dieter Landes, and Andreas Hotho. A survey of network-based intrusion detection data sets. Computers & Security, 86:147–167, 2019.

[154] A. M. Riyad, M. S. Irfan Ahmed, and R. L. Raheemaa Khan. An adaptive distributed intrusion detection system architecture using multi agents. International Journal of Electrical and Computer Engineering, 9(6):4951–4960, 2019.

[155] Dorothy Elizabeth Robling Denning. Cryptography and data security. Addison-Wesley Longman Publishing Co., Inc., 1982.

[156] Rodrigo Roman, Jianying Zhou, and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10):2266–2279, 2013.

[157] Antony Rowstron and Peter Druschel. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), volume 2218, pages 329–350. 2001.

[158] S J Russell and P Norvig. Artificial Intelligence: A Modern Approach Prentice Hall. New Jersey, 1995.

[159] Jake Ryan, Meng-Jang Lin, and Risto Miikkulainen. Intrusion detection with neural networks. In Advances in neural information processing systems, pages 943–949, 1998.

[160] Jean-Marc Seigneur, Adam Slagell, Jean-Marc Seigneur, and Adam Slagell. Collaborative Computer Security and Trust Management. Information Science Reference, 2010.

[161] D Selvamani and V Selvi. An efficacious intellectual framework for host based intrusion detection system. Procedia Computer Science, 165:9–17, 2019.

[162] Jaydip Sen. A Distributed Intrusion Detection System Using Cooperating Agents. arXiv preprint, nov 2011.

[163] Shahaboddin Shamshirband, Samira Kalantari, Z Sam Daliri, and Liang Shing Ng. Expert security system in wireless sensor networks based on fuzzy discussion multi-agent systems. Scientific Research and Essays, 5(24):3840–3849, 2010.

[164] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi. A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1):41–50, 2018.

[165] Ahmed F. Shosha, Pavel Gladyshev, Shinn-Shyan Wu, and Chen-Ching Liu. Detecting cyber intrusions in SCADA networks using multi-agent collaboration. In 2011 16th International Conference on Intelligent System Applications to Power Systems, pages 1–7. IEEE, sep 2011.

[166] Zhai Shuang-Can, Hu Chen-jun, and Zhang Weiming. Multi-agent distributed intrusion detection system model based on BP neural network. International Journal of Security and its Applications, 8(2):183–192, 2014.

[167] Abhishek Singh, Ola Nordström, Chenghuai Lu, and Andre LM Dos Santos. Malicious icmp tunneling: Defense against the vulnerability. In Australasian Conference on Information Security and Privacy, pages 226–236. Springer, 2003.

[168] Ankush Singla and Elisa Bertino. How Deep Learning Is Making Information Security More Intelligent. IEEE Security and Privacy, 17(3):56–65, 2019.

[169] Steven R. Snapp, James Brentano, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt, Biswanath Mukherjee, Stephen E. Smaha, Tim Grance, Daniel M. Teal, and Doug Mansur. DIDS (Distributed intrusion detection system) - Motivation, architecture, and an early prototype. Proceedings of the 14th national computer security conference, pages 1–9, 1991.

[170] Krzysztof Socha and Marco Dorigo. Ant colony optimization for continuous domains. European Journal of Operational Research, 185(3):1155–1173, mar 2008.

[171] Eugene H Spafford and Diego Zamboni. Intrusion detection using autonomous agents. Computer Networks, 34(4):547–570, oct 2000.

[172] Gary Stein, Bing Chen, Annie S. Wu, and Kien A. Hua. Decision tree classifier for network intrusion

detection with GA-based feature selection. In Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43, volume 2, page 136, New York, New York, USA, 2005. ACM Press.

[173] Nasrin Sultana, Naveen Chilamkurti, Wei Peng, and Rabei Alhadad. Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 12(2):493–501, mar 2019.

[174] Sung-Bae Cho. Incorporating soft computing techniques into a probabilistic intrusion detection system. IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews), 32(2):154–160, may 2002.

[175] K. S. Tang, K. F. Man, S. Kwong, and Q. He. Genetic algorithms and their applications. IEEE Signal Processing Magazine, 13(6):22–37, 1996.

[176] Tuan A. Tang, Lotfi Mhamdi, Des McLernon, Syed Ali Raza Zaidi, and Mounir Ghogho. Deep learning approach for Network Intrusion Detection in Software Defined Networking. Proceedings - 2016 International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking, pages 258–263, 2016.

[177] Shaohua Teng, Naiqi Wu, Haibin Zhu, Luyao Teng, and Wei Zhang. Svm-dt-based adaptive and collaborative intrusion detection. IEEE/CAA Journal of Automatica Sinica, 5(1):108–118, 2017.

[178] Abebe Tesfahun and D. Lalitha Bhaskari. Effective Hybrid Intrusion Detection System: A Layered Approach. International Journal of Computer Network and Information Security, 7(3):35–41, feb 2015.

[179] Rajendra Tiwari and R Gour. Mobile agent based distributed intrusion detection system: A survey. International Journal of Computer Applications in Engineering Sciences, 2, 2012.

[180] Trushna Tushar Khose Patil; and C.O.Banchho. A survey on Mobile Agent Based Intrusion Detection System. International Journal of Advanced Research in Computer and Communication Engineering, 1:773–777, 2012.

[181] E. Turban and J.E. Aronson. Expert Systems and Intelligent Systems. Prentice Hall, page 865, 2001.

[182] Esko Ukkonen. Algorithms for approximate string matching. Information and Control, 64(1-3):100–118, jan 1985.

[183] Emmanouil Vasilomanolakis, Shankar Karuppayah, Max Mühlhäuser, and Mathias Fischer. Taxonomy and survey of collaborative intrusion detection. ACM Computing Surveys (CSUR), 47(4):1–33, 2015.

[184] J. J. Verbeek, N. Vlassis, and B. Kröse. Efficient Greedy Learning of Gaussian Mixture Models. Neural Computation, 15(2):469–485, feb 2003.

[185] Theuns Verwoerd and Ray Hunt. Intrusion detection techniques and approaches. Computer communications, 25(15):1356–1365, 2002.

[186] Richard A VIGNA, Giovanni et KEMMERER. NetSTAT: A network-based intrusion detection system. Journal of computer security, 7(1):37–71, 1999.

[187] Stefan Voß, Silvano Martello, Ibrahim H Osman, and Catherine Roucairol. Meta-heuristics: Advances and trends in local search paradigms for optimization. Springer Science & Business Media, 2012.

[188] Ajinkya Wankhade and K. Chandrasekaran. Distributed-Intrusion Detection System using combination of Ant Colony Optimization (ACO) and support vector machine (SVM). Proceedings - 2016 International Conference on Micro-Electronics and Telecommunication Engineering, ICMETE 2016, pages 646–651, 2016.

[189] Hervé; WESPI, Andreas; DACIER, Marc; DEBAR. Intrusion detection using variable-length audit trail patterns. In: International Workshop on Recent Advances in Intrusion Detection. Springer, Berlin, Heidelberg, 1907:110–129, 2000.

[190] Danny Weyns, Elke Steegmans, and Tom Holvoet. Protocol-based communication for situated multi-agent systems. Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS 2004, 1:118–125, 2004.

[191] Benjamin Wilken and Massimiliano Antonio Poletto. Connection based detection of scanning attacks, May 11 2010. US Patent 7,716,737.

[192] Michael Wooldridge and Nicholas R Jennings. Intelligent agents: Theory and practice. The knowledge engineering review, 10(2):115–152, 1995.

[193] Shelly Xiaonan Wu and Wolfgang Banzhaf. The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing, 10(1):1–35, jan 2010.

[194] Sun Wu, Udi Manber, Gene Myers, and Webb Miller. An O(NP) sequence comparison algorithm. Information Processing Letters, 35(6):317–323, sep 1990.

[195] Akira Yamada, Yutaka Miyake, Keisuke Takemori, Ahren Studer, and Adrian Perrig. Intrusion detection for encrypted web accesses. In 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), volume 1, pages 569–576. IEEE, 2007.

[196] Jianhua Yang and Shou-Hsuan Stephen Huang. Matching TCP/IP packets to detect stepping-stone intrusion. International Journal of Computer Science and Network Security, 6(4):269–276, 2006.

[197] Liu Hua Yeo, Xiangdong Che, and Shalini Lakkaraju. Understanding Modern Intrusion Detection Systems: A Survey. arXiv preprint arXiv:1708.07174, 2017.

[198] Jaehak Yu, Hansung Lee, Myung-Sup Kim, and Daihee Park. Traffic flooding attack detection with snmp mib using svmq. Computer Communications, 31:4212–4219, 2008.

[199] Yuening Zhang, Yiming Zhang, Nan Zhang, and Mingzhong Xiao. A network intrusion detection method based on deep learning with higher accuracy. Procedia Computer Science, 174:50–54, 2020.

[200] Zheng Zhang, Scott Schwartz, Lukas Wagner, and Webb Miller. A Greedy Algorithm for Aligning DNA Sequences. Journal of Computational Biology, 7(1-2):203–214, feb 2000.

[201] Chenfeng Vincent Zhou, Christopher Leckie, and Shanika Karunasekera. A survey of coordinated attacks and collaborative intrusion detection. Computers & Security, 29(1):124–140, 2010.

[202] Man Zhou, Lansheng Han, Hongwei Lu, and Cai Fu. Distributed collaborative intrusion detection system for vehicular ad hoc networks based on invariant. Computer Networks, page 107174, 2020.

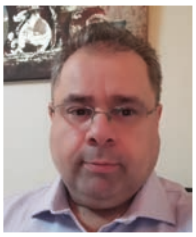
Nassima Bouguerou, she received her Bachelor and the Master degrees both in computer science from the University of Skikda, Algeria in 2010 and 2012, respectively. She is now and since 2013 a Ph.D. student within the department of computer science of the same university. Her research interests include network security, distributed systems and deep learning modeled as multi-agent systems in intrusion detection systems.

Smaine Mazouzi, he is a professor of computer science at 20 aout 1955 university of Skikda. He received his M.S. and Ph.D. degrees in Computer Science from university of Constantine, respectively in 1996, and 2008. His fields of interest are pattern recognition, machine vision, and computer security. His current research concerns using distributed and complex systems modeled as multi-agent systems in image understanding and intrusion detection. He is interested also in distributed machine learning and distributed meta-heuristics and their application to computer security and image processing.

Mohamed Belaoued, completed his Master's, and Ph.D. degrees in computer science at the University of Skikda, in 2011, and 2016, respectively. In 2016, he joined the University of Constantine 1, where he held the position of Assistant then Associate Professor for three years. He is currently an associate professor at the University of Skikda, Algeria, and a researcher with LICUS laboratory at the department of computer science of the same university. He is also a member of the Global Foundation for Cyber Studies and Research (GFCYBER). His research interests include malware analysis and detection, intrusion detection, networks and IoT security.

Noureddine Seddari, holds M.S. and Ph.D. degrees in Computer Science from the University of 20 August 1955-Skikda, Algeria, in 2011 and 2015, respectively. He is currently an Associate Professor of Computer Science at the same University. He was an associate teacher and researcher at the University of Abdelhamid Mehri, Constantine, Algeria, from 2015 to 2017. He is membre of the LICUS laboratory at the Department of Computer Science of the University of Skikda. His current research interests include agent oriented software engineering, artificial intelligence, Fake news detection, malware detection, DEVS formalism, multi-formalism modelling and computer simulations.

Abdelouahid Derhab, Received the Engineering, master's, and Ph.D. degrees in computer science from the University of Sciences and Technology Houari Boummediene, Algiers,in 2001, 2003, and 2007, respectively. He was a full-time Researcher with the CERIST Research Center, Algeria, from 2002 to 2012. He is currently an Associate Professor with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia. His research interests include network security, intrusion detection systems, malware analysis, mobile security, and mobile networks.



Prof. **Abdelghani Bouras** holds a Ph.D. in operations research, from Joseph Fourier University, Grenoble. He is an engineer and master of operations research. He is currently a Professor of Industrial Engineering at Al Faisal University, Riyadh. He was formerly a Professor of Industrial Engineering at Ecole Centrale Casablanca and King Saud University. He worked as an associate professor of operations management and quantitative methods at the School of Business and Administration at Al Akhawayn University in Ifrane (AUI), and as an assistant professor of production management at the School of Business and Management at Liege University. He worked in industry as an operations research analyst at Usinor-Arcelor Group (steel industry), as a modeler-Analyst for Electrabel-Suez group (Belgian electricity producer), and finally as a consultant for Pechiney (Aluminium industry). He is involved in many types of research in mathematical modeling, operations research, operations & supply chain management.