Computer Networks 160 (2019) 165–191

Contents lists available at ScienceDirect

Computer Networks

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

Review article

Intrusion detection systems in the Internet of things: A comprehensive investigation

Somayye Hajiheidari[a], Karzan Wakil[b], Maryam Badri[c], Nima Jafari Navimipour[d,*]

[a] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran
[b] Research Center, Sulaimani Polytechnic University, Sulaimani 46001, Kurdistan Region, Iraq
[c] Department of Electrical Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran
[d] Young Researchers and Elite Club, Islamshahr Branch, Islamic Azad University, Islamshahr, Iran

ARTICLE INFO

Article history:
Received 26 December 2017
Revised 16 May 2019
Accepted 16 May 2019
Available online 17 May 2019

Keywords:
Internet of things
Intrusion detection
Internal attack
Anomaly detection
Signature
Distribution

ABSTRACT

Recently, a new dimension of intelligent objects has been provided by reducing the power consumption of electrical appliances. Daily physical objects have been upgraded by electronic devices over the Internet to create local intelligence and make communication with cyberspace. Internet of things (IoT) as a new term in this domain is used for realizing these intelligent objects. Since the objects in the IoT are directly connected to the unsafe Internet, the resource constraint devices are easily accessible by the attacker. Such public access to the Internet causes things to become vulnerable to the intrusions. The purpose is to categorize the attacks that do not explicitly damage the network, but by infecting the internal nodes, they are ready to carry out the attacks on the network, which are named as internal attacks. Therefore, the significance of Intrusion Detection Systems (IDSs) in the IoT is undeniable. However, despite the importance of this topic, there is not any comprehensive and systematic review about discussing and analyzing its significant mechanisms. Therefore, in the current paper, a Systematic Literature Review (SLR) of the IDSs in the IoT environment has been presented. Then detailed categorizations of the IDSs in the IoT (anomaly-based, signature-based, specification-based, and hybrid), (centralized, distributed, hybrid), (simulation, theoretical), (denial of service attack, Sybil attack, replay attack, selective forwarding attack, wormhole attack, black hole attack, sinkhole attack, jamming attack, false data attack) have also been provided using common features. Then the advantages and disadvantages of the selected mechanisms are discussed. Finally, the examination of the open issues and directions for future trends are also provided.

1. Introduction

Connectivity of physical things to the Internet makes it possible to control and manage them from a distance [1]. These devices sense and record client activities, forecast their future actions and give him/her the useful services [2]. It is anticipated that, in the next decade, the Internet will be a seamless fabrication of common networks and related objects [3]. The IoT [4] as a new term in data and information age was originally introduced by the MIT Auto-ID Center in 1998 [5]. It represents a vision where objects are exclusively identified and available over the Internet [4,6,7]. Also, the real world can be more available through personal computers and networked devices over the IoT and Internet [8,9]. US National Intelligence Council (NIC) believes that IoT has a potential effect on US national power. So, they have decided to put it on the list of six disruptive civil technologies [10,11]. NIC tries to insert Internet nodes in everyday things by 2025, including food parcels, furniture, paper documents, and more.

By rapid development of the IoT, its security has been taken into consideration and turned into the most challenging topics in such a connecting and mutual framework [12,13]. Hackers, malicious software, and viruses might frustrate data and their integrity. Also, insecurity of data may specifically reduce the security of whole IoT and brings many risky situations [14,15]. Furthermore, many communications in the wireless environment provide the ease of eavesdropping effortlessly [16]. Therefore, security converts to a hot topic in the IoT. Existing security techniques include systemic security structures and cryptography security mechanisms. The threat of network attacks, such as the volume of requests to the IoT services in a very short time interval or the existences of the unauthorized access to some services may cause drastic disasters [17]. Therefore, in order to detect the intruders, the use of IDSs is necessary for keeping the IoT networks secure and accessible. However, because of the sources and energy limitations of the IoT devices, it is rarely possible to operate the complex IDSs in this

* Corresponding author.
E-mail address: jafari@iaut.ac.ir (N.J. Navimipour).

https://doi.org/10.1016/j.comnet.2019.05.014
1389-1286/

environment. An IDS examines the status and behavior of a network. When an intrusion is detected, an alert is triggered and the network administrator is able to respond based on the alert issued [16]. The architecture of traditional IDSs is mainly for the priority management characteristics of the Internet, which lacks in the aspects of control and management of real-time, especially in various volumes and improper sequences of event streams [18–21]. There are primarily four types of IDSs. The first type is signature-based IDS which describes patterns of each type of attack that the IDS should detect. An alert will rise when suspicious behavior matches the pattern. This is a simple method which can detect known attack effectively [22,23]. Anomaly-based IDS has a start-up stage where it collects data about the normal behavior of the observed system. After that, it determines a threshold that if it is exceeded by a suspicious behavior, the IDS raises an alarm. This technique can detect unknown attacks, but it suffers from computationally cost and needs abundant memory for data analysis [24,25]. Also, a hybrid of the anomaly and signature-based IDS try to create a tradeoff between the storage cost of the signature-based and the computing cost and false positive alarms issue of the anomaly-based detection mechanism [26]. The specification-based IDS specifies the usual system operations and verify the current operations based on the specified operations [27]. As it is evident, the papers which are surveyed in this review are not capable of detecting all type of attacks so they focus on specific types of attacks. Then they have been categorized in different categories according to attacks that they can detect. These categories are a denial of service attack, Sybil attack, replay attack, selective forwarding attack, wormhole attack, black hole attack, sinkhole attack, jamming attack, false data attack which will be explained in detail in Sections 3–4 below.

To simplify the use of IDSs in the IoT and further identification of weaknesses and strengths of these systems, it is important to systematically review the existing literature and articles. In contrary to the importance of IDSs in the IoT, there is not any comprehensive and wide-ranging systematic review of these mechanisms. Therefore, this paper widely analyzes all the literature between the years 1998 and 2018 systematically, because the term of IoT is proposed for the first time in 1998. Four categories are performed to adjust the review: (1) anomaly-based, (2) signature-based, (3) specification-based and, (4) hybrid IDSs. Categorizing the existing IDSs in the IoT, comparison of different intrusion detection techniques, and summary of the upsides and downsides of the reviewed IDSs are considered in this paper to study and evaluate the works. Then, future guidelines are prepared for researchers regarding the application of IDSs in the IoT. To achieve this goal, digital libraries are searched and 50 studies are determined. Briefly, the purposes of this paper are as follows:

- Providing an overview of the current challenges related to IoT that can be addressed in the IDS.
- Providing a Systematic Literature Review (SLR) of the current techniques of IDS and the way wherein these have been applied to the IoT.
- Exploring the future challenges about the role of IDS in the IoT.
- Outlining the key ranges where future investigation can advance the use of the IDSs in the IoT.

The rest of the paper is organized as follows: Section 2 demonstrates the related survey and overview the papers which are about the IDSs. Section 3 includes a brief discussion about related technologies, which are used in the article. Section 4 discusses the research questions. Section 5 demonstrates the examination of the acquired results and presents the answers to the research questions by identifying the intrusion detection metrics. The discussion of the IDSs and the comparison of the selected techniques in the IoT are demonstrated in Section 6. Section 7 gives the open issues and future trends identified with the IDS in the IoT. The limitations of the paper are discussed in Section 8. Eventually, the conclusion is presented in Section 9.

2. Related work

Many types of survey and review researches have been done in the field of intrusion detection on the network, Wireless Sensor Networks (WSN) [28], cloud computing [29,30], and other areas. However, there is not any systematical literature survey that refers directly to the intrusion detection techniques in the IoT. Some survey papers in the field of IDS are studied in this section to highlight the need for reviewing the IDS mechanisms on the IoT.

Using genetic algorithm-based approaches for IDS has been reviewed by Owais et al. [31]. The paper demonstrates how genetic algorithms are effectively used as a part of IDS. The paper shows that the genetic algorithm can detect normal behavior from abnormal behavior via intrusion detection. Generating the related rules and using them to filter new connections and specify doubtful network traffic are considered as the goal of a genetic algorithm [32]. The paper additionally demonstrates that the genetic-based strategies are realized effectively in IDS in an offline learning framework. In the real-time IDS, some rules are employed to arrange the received network connections in the progressive environment. However, the survey is not an SLR, therefore, the articles selection process has not been stated. Further, there is not any classification of existing techniques in the survey. Also, since the paper was published in 2008, the newly proposed papers are not included in this paper.

Wang et al. [33] have reviewed the basic idea of the Hidden Markov Model (HMM)-based IDS. In their survey, different optimization parameters of IDS such as efficiency, speed, and precision have been examined. They have stated that efficient HMM training is important for anomaly-based IDS. Also, they have shown that recent researches have focused on fast and effective HMM training without reducing accuracy. Similar to the previous review, the survey is not an SLR because the selection process of articles has not been stated. Also, there is not any classification of existing techniques in the survey. Since the paper was published in 2008, it does not include newly proposed papers.

Furthermore, Helali [34] has demonstrated the structures of a signature-based technique for IDS using data mining scheme. Data mining has turned into an exceptionally helpful procedure to lessen data overload. Some techniques are also employed for classification and pattern recognition which has been broadly utilized as a part of separating normal from anomaly behavior. The paper demonstrates that data mining can be effectively utilized as a part of the configuration of IDS. Like the previous articles, the paper is not an efficiently surveyed paper on these fields where the determination procedure of articles has not been expressed. Since the paper was published in 2010, the latest published papers in the IoT environments are not included.

Moreover, Kolias et al. [35] have exhibited the use of swarm intelligence in IDS. A major contribution of the paper is to provide a comparison of some swarm intelligence-based IDS techniques in terms of efficiency. Parallel nature of these methods could decrease the training time and increase the quality of the IDS. They have shown that a large portion of the swarm intelligence-based IDSs endures high calculations and a high number of cycles (through the setting of particular parameters) to decrease the performance. Both of these variables negatively affect the prerequisites of the framework regarding computational cost. Like other reviewed articles, this article reviews the IDSs in the general systems and it is not a precise writing survey on the IoT field. Also, the procedure of selecting articles has not been expressed. In addition, the paper

was published in 2011 and it does not include recently published papers.

Sherasiya et al. [36] have provided a survey on the IDS for IoT. In this paper, some potential security attacks are made in the IoT applications and various intrusion detection approaches to mitigate those attacks are proposed. The paper mentions that those approaches cannot be able to detect all kinds of cyber-attacks and are not feasible for the IoT network because it has high power, storage, and bandwidth consumption for intrusion detection. However, this article discusses the IDSs in the IoT, but it surveys only a few numbers of articles. Further, the process of selecting the articles has not been demonstrated.

Gendreau and Moorman [37] have proposed a review of the IDS techniques in the IoT. The survey starts with a historical investigation of IDSs in order to understand the IDS platform. This investigation of the basis of IDS research based on the modules of the IoT is followed by a look at the current general process and an examination of these methods. Lastly, guidelines for potential IDS in the IoT are mentioned before identifying the open research problems. Similar to the former study, this paper surveys a few numbers of articles. Also, the article selection process has not been mentioned.

Zarpelão et al. [38] have demonstrated a survey of IDS techniques which are proposed for IoT. The purpose of the article is to highlight the leading trends, open issues, and future trends. The proposed IDSs have been classified in some categories according to the following attributes: detection method, IDS placement strategy, security threat, and validation strategy. However, the process of selecting articles has not been demonstrated and the recently proposed articles are not investigated.

Borgohain et al. [39] have demonstrated a general review of the security problems in the IoT along with an investigation of the privacy issues that an end-user might confront as a result of the deployment of IoT. The main focus is on the security weak points creating out of the information exchange technologies used in IoT. No counteractions to the security bugs have been investigated in the paper. The survey is not an SLR, therefore, the articles selection process has not been stated. Further, there is not any classification of existing techniques in the survey. Also, the newly proposed papers are not included in this paper.

Ammar et al. [40] have proposed a review of the security of the fundamental IoT structures. For every framework, creators clear up the proposed system, the fundamentals of developing third-party smart applications, the compatible hardware, and the security highlights. Similar to other mentioned papers, the selection process of the papers is not presented. Also, recently published papers are not included in this review.

Yang et al. [41] have exhibited the security and privacy problems in IoT applications and frameworks. They have introduced the restrictions of IoT objects in battery and computing resources. They also have talked about extending the battery life and lightweight computing. They likewise have contemplated existing classification approaches for IoT attacks and security instruments. According to the authors claim, recently demonstrated IoT authentication methods and systems up to 2017 have been audited. The last piece of the work examined the security issues and solutions in four layers, including the perception layer, network layer, transport layer, and application layer. The overview incorporates four sections. The initial part will investigate the most significant restrictions of IoT objects and their solutions. The second one will introduce the classification of IoT attacks. The next part will concentrate on the systems and structures for authentication and access control. The last part will investigate the security issues in various layers. However, the process of selecting the articles are ambiguous and is not mentioned.

Kouicem et al. [42] have provided a comprehensive top-down survey of the security and privacy methods in the IoT. They have studied especially the benefits of new approaches such as blockchain and Software Defined Networking (SDN) which can bring to the security and the privacy components of IoT in terms of flexibility and scalability. Finally, they have given a public classification of existing solutions and comparison based on important parameters. However, the process of selecting articles is ambiguous.

Most of the published articles have ignored many of the reputable articles. None of the reviewed articles used an SLR, so the selection process of the articles is so vague without any suitable order. Also, the newly published papers in the IoT environment are not evaluated in some of the evaluated papers. Therefore, it is crucial to pay attention that the present study is superior to the published articles due to the process of selecting articles, the study of valid and different databases and the number of reviewed articles.

3. Backgrounds

The related technologies, which are used in this article, are briefly discussed in this section.

3.1. Commonly used metrics

Appropriate IDS is helpful in enhancing the accuracy of detection, decreasing the false alarm rate, improving resource utilization, and also detecting attacks with low delay. Some metrics are very important in evaluating the efficiency of the IDSs, which are explained as follows:

Detection accuracy: It is the number of malicious nodes, which is effectively identified against the total number of malicious nodes in the network [26].

False positive rate: It is characterized by the rate of normal traffic that are mistakenly distinguished as malicious [43]. The intrusion detection module inaccurately distinguishes a normal action as suspicious [44].

Resource consumption: It is the difference between the numbers of resources that are requested before the system operation with the number of resources that are released when its operation ends [45].

Real-time intrusion detection: It is a system that can unceasingly monitor the system and clients behavior to detect doubtful behavior as, or soon after, it occurs [46].

Flexibility: The flexibility is the ability of a network to adapt and continue when new conditions happen [47].

Scalability: The ability of the IDS to continue operation against the system development and the ability to maintain the relative accuracy of detection [47].

3.2. Network structure

There are three types of IDS based on the network structure, including centralized, distributed, and hybrid. In the centralized IDS, the examination of the data is done in a fixed number of places, independent of how many hosts are being checked [48]. In these schemes, the IDS is placed in cluster head or border router in which the traffic of nodes is sent to the central IDS and then the IDS analyzes the traffic that has been gathered by sensors to detect the intrusions. Murynets and Jover [49] have proposed two algorithms for monitoring the traffic of the devices in the IoT network to detect anomalous behavior. The proposed methods are based on a centralized scheme in which sensor nodes do not interfere with the detection of attacks.

In distributed IDS (dIDS), the detection system is placed on the sensors of IoT networks; then after collecting the traffic of the environment, each of the sensors can detect the intrusion locally. In other words, a dIDS includes several IDSs in a large network, all of which are connected together or with a central server, which

makes it easy to monitor the network and investigate the occurrence of an attack [50].

The hybrid IDS is the combination of distributed and centralized techniques to take advantage of their strong points and avoid their drawbacks. IDS is placed in each sensor node and can detect intrusions locally. In addition, after detecting the intrusion on nodes, the located IDS in the border router node can detect intrusions globally. For example, Raza et al. [26], Matsunaga et al. [51] have proposed a hybrid scheme that IDS placed on the 6lowpan Border Router (6BR) and sensor nodes.

3.3. Types of attacks

Many well-known types of attacks which can be detected by IDSs are briefly discussed in this section.

- DoS attack: Presence of each attack such as DoS/DDoS can disorder the usability of the networks by sending data in particular samples over the network, or by simply flooding packets. It is often possible for attackers to hinder the remote service [52].
- Sybil attack: In this type of attack, an adversary presents faked identities to legitimate nodes. An adversary may make such identities with disabling the legitimate nodes permanently [53,54].
- Replay attacks: In the first step, the attacker performs an intrusion from time t_0 until t_n and collect data, then replaying the collected data [55].
- Selective forwarding attack: In selective forwarding attacks, some of the specified packets (not every packet) are refused to forward or dropped by the malicious attacks. The adversary ensures that the packets are never propagated [56].
- Sinkhole attack: In a sinkhole attack, attracting the data from all neighboring nodes is the goal of the compromised node [57].
- Wormhole attack: An attacker gets the packets at the one side of the network, tunnels them to another side, then relays them into the network from that point [57].
- Black hole attack: In the black hole attack, an attacker listens to the request packets using the dynamicity of the routing protocol in order to abuse it by replying with a faked reply packet [58].
- Jamming attack: In jamming attacks, attacker firstly keeps monitoring wireless medium to control the frequency of receiving a signal from the sender by the destination node [57]. Secondly, it transmits a signal on that frequency so that the fault-free receptor is hindered [57].
- False data attack: Finally, in the false data attacks, the attacker defines the present organization of the network, then, it inserts destructive measurements that will misguide the state estimation procedure without being distinguished by the used methodologies [59].

4. Systematic literature review

An SLR is a serious examination to estimate all exploration studies and papers that mention a specific topic. In the systematic review, a description of the finding method of research papers is presented [60,61]. Errors have been limited, chance effects have been reduced and the quality of data analysis has been improved [62,63]. The benefits mentioned above lead to reliable results and an appropriate conclusion [64]. It is originated from the field of medication and studies about the fields of engineering and sociology have started using this method, recently [65]. Therefore, in this section, it is employed to do a complete and systematic study of the important methods in the field of IDS in the IoT environment.

4.1. Method

In the SLR, the planning, conducting, and reporting process is done via the techniques that have been demonstrated in [66,67]. Also, the presented methods for SLR in [68,69] are considered and some techniques of them are used in this paper. Fig. 1 exhibits the required steps in the SLR. First, the need for a systematic review is identified to assess the use of IDSs in the IoT. Also, the weaknesses and strength of the existing methods are determined. In order to improve the functionality of the IDSs in the IoT environment, the research issues have also been demonstrated. Next, the research questions are defined. Then the research methodology, which contains specifying of search phrases and sources choosing are

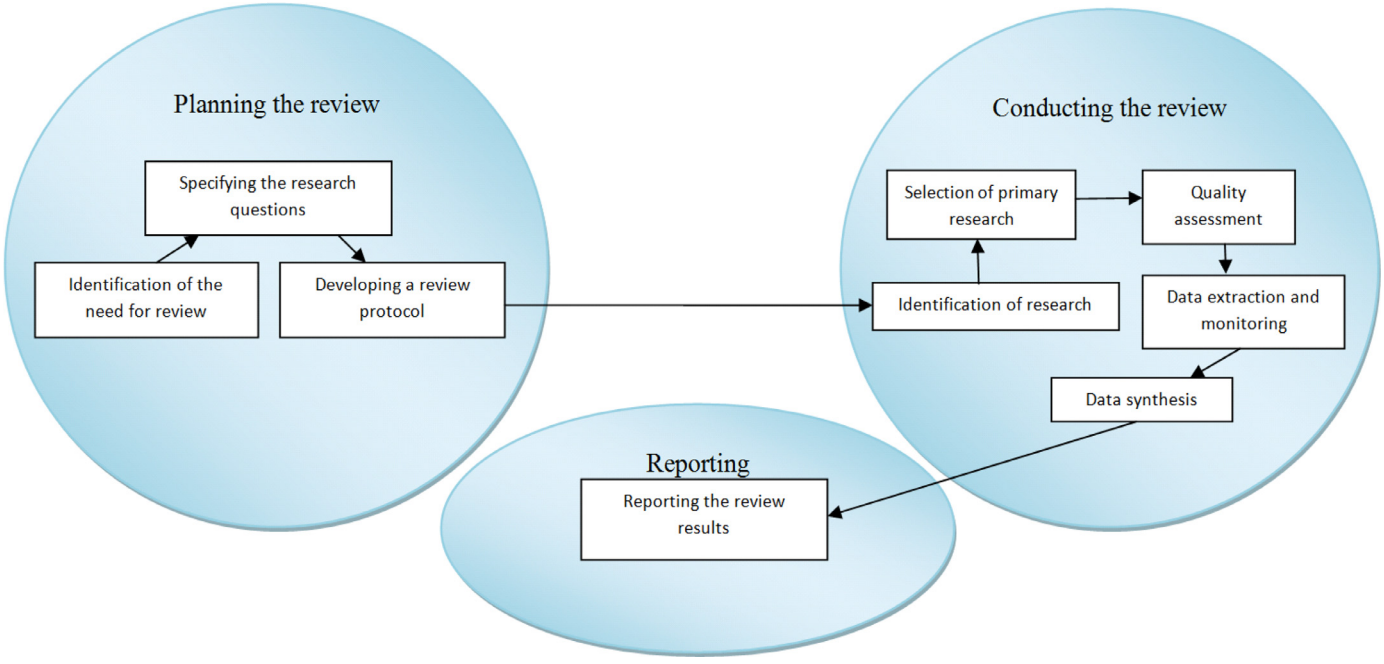

Fig. 1. Research method.

Table 1
Research questions.

RQ#	Research questions	Motivation
RQ1	Which IDSs have been used in the IoT?	Identifying IDS techniques normally being used in the IoT.
RQ2	Which anomaly detection techniques have been used in the IoT?	Identifying the anomaly detection techniques commonly being used in the IoT.
RQ3	Which signature-based detection techniques have been used in the IoT?	Identifying the signature-based intrusion detection techniques commonly being used in the IoT.
RQ4	Which metrics are commonly used for intrusion detection in the IoT?	Evaluating the existing IDSs based on the primary IDS metrics in the IoT.
RQ5	How much the existing intrusion detection approaches meet the main metrics?	Evaluating the existing intrusion detection approaches based on the main metrics in the IoT.
RQ6	What are the main advantageous and disadvantageous of the IDSs in the IoT?	Determining the information about IDSs in the IoT.

identified. In the next step, related studies are determined based on the study questions. In this step, the inclusion and exclusions criteria are also defined. Then the quality evaluation scale is determined by forming a quality evaluation questionnaire for analyzing and evaluating the studies. The next step includes the designing of data extraction to synthesize the necessary information and answer the research questions. Finally, a method for data synthesis and reporting the review results are designed. The research questions are clarified in the following subsection.

4.2. Research questions

Evaluating the empirical proof of the IDS components in the IoT is the goal of this section. Table 1 shows six research questions related to this systematic literature review.

4.3. Search strategy and study selection

Search strings are determined by providing the synonyms and alternative spellings for each of the questionable terms and associate them using the Boolean OR and Boolean AND. Hence, five keywords have been selected including “intrusion detection system”, “anomaly detection”, “signature detection”, “internal attack”, and “Internet of things”. The following search terms are used for selecting of main studies (intrusion AND detection AND ((internet AND things) OR IoT)) OR (anomaly AND detection AND ((internet AND things) OR IoT)) OR (signature AND detection AND ((internet AND things) OR IoT)) OR (internal AND attack AND ((internet AND things) OR IoT)). After recognizing the search terms, the related and significant digital databases are selected. This study is based on the articles have been found in the electronic databases, which are exhibited in Table 2 [70,71].

The search is made in the mentioned 14 electronic databases by means of the target search string. The search is restricted from 1998 to 2018 since the IoT was launched in 1998s. After identifying the candidate found papers, the full-text of the relevant papers, are obtained. The practical studies are included using the IDS in the IoT. 281 primary studies are identified for inclusion in the SLR. Then, the references of the selected studies have been investigated and more than 57 studies are identified for further processing and analysis. This step is exhibited in stage 1 in Fig. 2. After the inclusion and exclusion criteria, which are given in Table 3, 183 papers are picked up to further evaluation in the next stage.

Table 2
Electronic databases used in the applied systematic literature review.

Online databases#	Online database	URL
1	IEEE	http://ieeexplore.ieee.org/
2	ScienceDirect	http://www.sciencedirect.com/
3	ACM	http://www.acm.org/
4	Wiley	http://www.wiley.com/
5	Google Scholar	https://scholar.google.com/
6	SpringerLink	http://link.springer.com/
7	Emeraldinsight	http://emeraldinsight.com/
8	Sagepub	https://uk.sagepub.com/
9	Scientific	http://www.scientific.net/
10	DOAJ	https://doaj.org/
11	Taylor and Francis	http://taylorandfrancis.com/
12	Inderscience	http://www.inderscience.com/
13	MDPI	http://www.mdpi.com/
14	Hindawi	https://www.hindawi.com/

4.4. Quality assessment criteria

The quality questions have been provided in Table 4. The quality assessment is employed for weighing the studies. Table 4 presents the quality assessment questions. The questions are ranked 1 (yes), and 0 (no) and the final score is attained by adding the values allocated to each question and only the studies with two yes answers are selected to include in the review. At the end of this step, 43 studies are chosen, which are reviewed in this paper in Section 5. Also, this step is shown in stage 3 in Fig. 2.

4.5. Results and discussion

For data analysis, the author name, title, publishing particulars, simulation details, and the proposed scheme are summarized. Then the data extraction is utilized to gather obtained information from the articles. The outcome is saved for use in the data synthesis procedure. The current review aims to analyze the selected articles to find answers to the questions raised. The quantitative data, which includes some metrics such as detection accuracy, false positive rate, resource consumption, real-time, flexibility, reliability, scalability are evaluated and scrutinized; then upsides and downsides of the IDSs, and categorization of various IDSs are proposed. Charts and tables have been used in order to answer the mentioned research questions and summarize the results of this review. The obtained results from the studies that have been selected for IDS in the IoT are shown in the rest of this subsection. In Section 4.5.1, the numbers of articles that have been published in 1998–2018 are investigated. Briefly, the first steps for selection of the articles after inclusion/exclusion are explained in Section 4.5.2.

4.5.1. Distribution of articles by publisher

Table 5 demonstrates the distribution of articles before applying inclusion/exclusion criteria that have been selected based on the considered keywords in the various databases. The table has three columns that the first one shows the years; the second column shows the various databases that papers are selected based on keywords. The third column demonstrates the number of articles, which are published in various databases. According to Table 5, the number of published papers in IEEE in 2015 has the maximum amount of papers compared to other publications in other

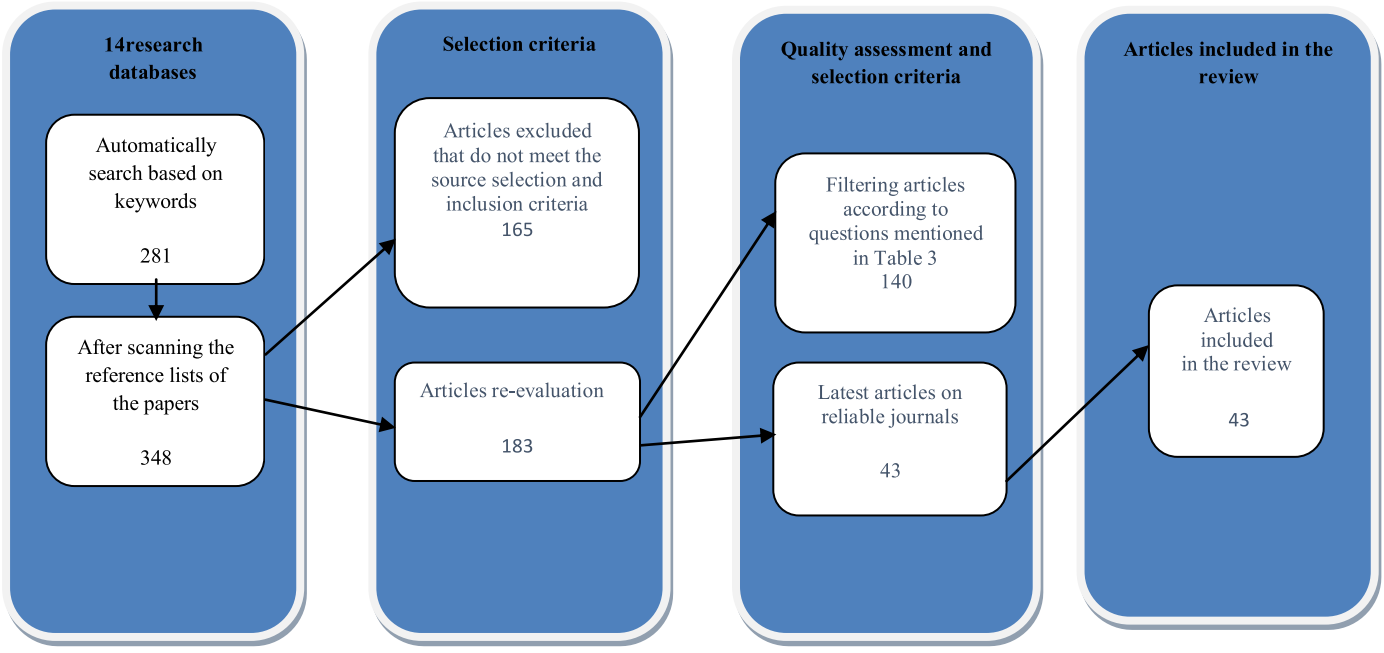

Fig. 2. The selection process of the articles in the form of a diagram.

Table 3
Summary of the inclusion-exclusion criteria for review protocol.

Criterion	Rational
Inclusion1: A study that clearly defines how the IDSs could be applied and assisted in the IoT environment.	We want to recognize how IDSs affect the security of the IoT, thus, we need the articles that directly propose the IDS in the IoT.
Inclusion2: A paper which is published by academics.	Both academic and industrial methods are important to this study.
Inclusion3: A study that is published in the IoT field.	IoT is our reference field.
Inclusion4: A study that is peer-reviewed.	A peer-reviewed paper assurance an assured level of quality and comprises a reasonable amount of content.
Inclusion5: A paper which contains journal and conference papers.	Master's and doctoral dissertations, textbooks, editorial notes, and unpublished working articles were omitted.
Exclusion1: A study that does not focus on intrusion detection techniques in the IoT environment	The emphasis of this paper is only on studies that present the IDSs exactly in the IoT.
Exclusion2: Review studies	Since the review studies are not presented with a new idea, they are excluded.
Exclusion3: Non-English papers	The papers that did not publish in the English are excluded.

Table 4
Summary of the quality assessment criteria for review protocol.

Q#	Quality Questions	Yes	No
Q1	Does the research paper have any simulation or evaluation of the proposed method?		
Q2	Does the selected conference paper belong to a valid publication?		

years. Fig. 3 shows that the number of papers before applying inclusion/exclusion criteria in Wiley, Taylor, Springer, Scientific, Elsevier, MDPI, IEEE, Hindavi, Emerald, ACM, and other publications are 6, 1, 26, 25, 26, 5, 160, 7, 1, 14 and 67, respectively. About 46% of the studies are published in IEEE.

4.5.2. Publication year

Fig. 4 demonstrates the distribution of the articles that have been selected by the keywords in the various databases by the year of publication before applying inclusion/exclusion criteria. The figure shows that the number of published articles in the journals and conferences from 2002 is increased. Fig. 4 also exhibits that before 2009, only 5 papers were published based on the search keywords. The number of studies during 2009–2018 are 9, 12, 22, 43, 50, 56, 62, 52, 13, 14, respectively. About 98% of the studies are between 2009 and 2018. Also, 2% of the articles are published before than 2009. A number of published articles in 2015 are 62 that is the maximum number of articles in 1998–2018. Fig. 4 also demonstrates that the number of papers is increasing during 2003–2015.

Fig. 5 exhibits the number of articles by year of publication after applying the inclusion/exclusion criteria. After doing inclusion/exclusion and quality assessment criteria on the selected papers, 43 papers have been selected in this review. Fig. 5 shows that during the years 2009–2018, 1, 2, 0, 4, 3, 8, 11, 10 and 4 papers are published in journals and conferences, respectively. The percentage of the articles based on publishers after applying the inclusion/exclusion criteria are shown in Fig. 6.

5. Intrusion detection systems

In order to respond to research questions, the selected studies are reviewed and the most frequently addressed IDSs is identified. There are various kinds of IDSs in the IoT such as signature-based, anomaly-based, specification-based, and hybrid IDS. They differ by their mechanism of discovering malicious nodes.

Table 5
Distribution of articles by the publisher before applying inclusion/exclusion criteria.

Year of publication	Publisher	Number of articles
2002	IEEE	2
2003	Other publications	1
2006	Springer	1
	ACM	1
2009	Springer	1
	IEEE	5
	MDPI	1
	Other publications	2
2010	Springer	2
	Scientific	1
	Science Direct	1
	IEEE	4
	MDPI	1
	Other publications	3
2011	Springer	3
	Scientific	2
	IEEE	13
	Other publications	4
2012	Wiley	3
	Springer	3
	Scientific	4
	ACM	4
	Hindavi	1
	IEEE	17
	Other publications	11
2013	Wiley	1
	Springer	3
	Scientific	9
	Science Direct	4
	ACM	4
	Hindavi	1
	IEEE	17
	Other publications	11
2014	Springer	2
	Scientific	7
	Science Direct	3
	ACM	3
	Hindavi	2
	IEEE	29
	MDPI	1
	Sagepub	1
	Other publications	8
2015	Springer	3
	Science Direct	7
	IEEE	37
	Other publications	15
2016	Wiley	2
	Taylor	1
	Springer	6
	Science Direct	6
	Emerald	1
	Hindavi	1
	IEEE	24
	Other publications	11
2017	Science Direct	3
	IEEE	5
	Hindavi	1
	Scientific	1
	MDPI	1
	ACM	2
2018	Science Direct	2
	IEEE	7
	Hindavi	1
	Scientific	1
	MDPI	1
	Springer	2

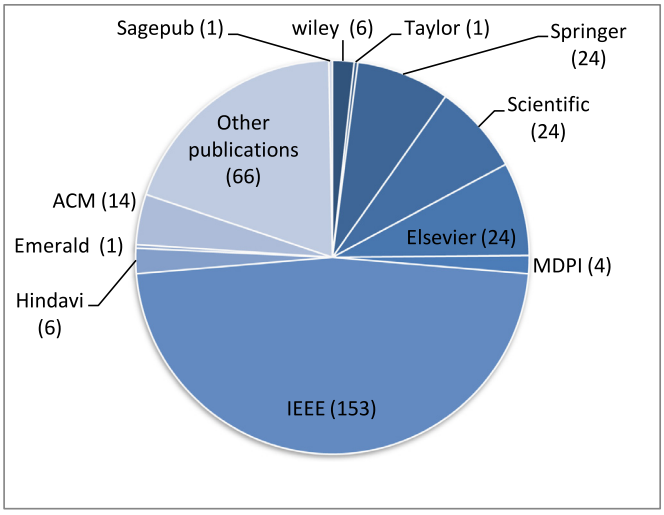

Fig. 3. Percentage of the articles based on publishers.

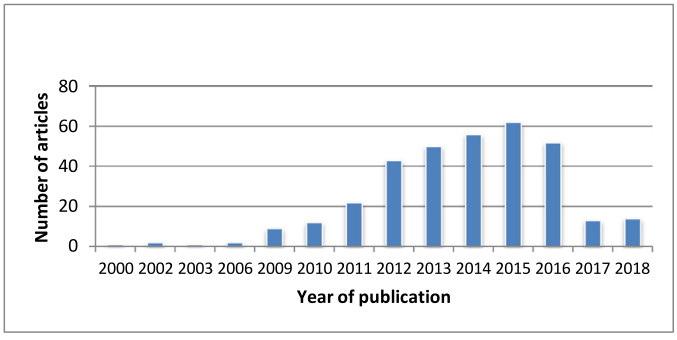

Fig. 4. Distribution of the articles by the year of publication before applying inclusion/exclusion criteria.

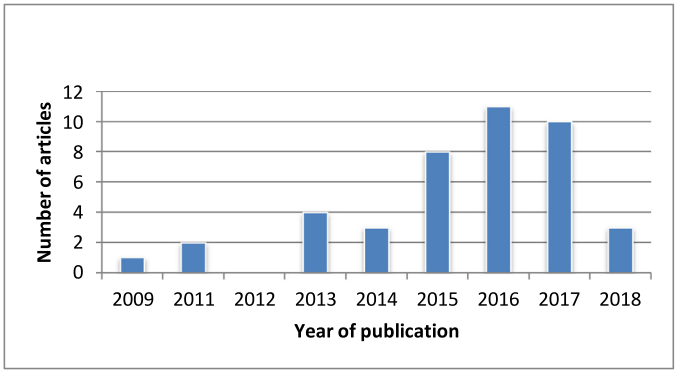

Fig. 5. Distribution of the articles by year of publication after applying the inclusion/exclusion criteria.

Fig. 7 shows the four types of IDS categorization. The first type is based on previously mentioned intrusion detection techniques. The second type is based on the location of IDS, including centralized, distributed, and hybrid. The third type is based on evaluation techniques such as simulation and theoretical. The fourth is based on potential attacks. The rest of this section provides the types of considered categorizations with classifying the selected papers in each category.

Fig. 8 shows the categorization of the selected studies in four groups, including anomaly-based, signature-based, specification-based, and hybrid IDSs. For each category, the selected papers are illustrated. In the rest of this section, the selected studies are dis-

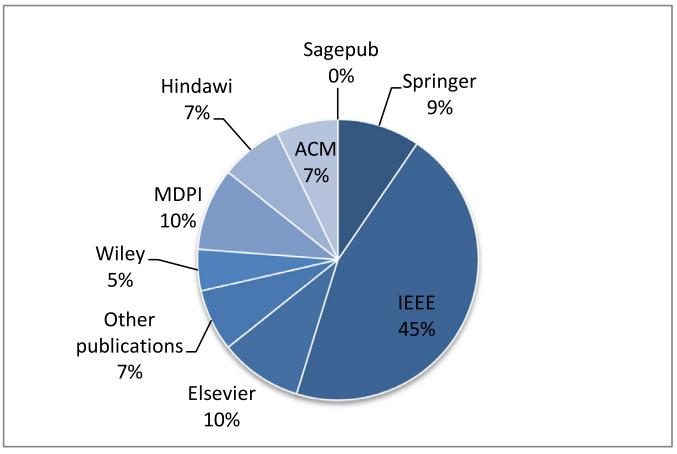

Fig. 6. Percentage of the selected articles based on the different publishers after applying the inclusion/exclusion criteria.

cussed and evaluated in four categories, including anomaly-based IDS, signature-based IDS, specification-based IDS, and hybrid IDS.

5.1. Anomaly-based IDS in the IoT

Anomaly-based IDS is used for detecting the intrusions and monitoring the misuse activity. It categorizes this activity as normal or abnormal with using threshold. In the IoT, these kinds of IDSs can monitor the behavior of the normal network to define a threshold. In order to detect the intrusions, the behavior of the network is compared with the threshold and any deviation from this value is considered anomaly [26]. In this section, the selected anomaly-based IDSs and their basic characteristics have been described and then compared in Table 6.

Fu et al. [16] have presented an IDS using anomaly mining. The intrusion semantic is examined to detect intrusions from anomalies. The proposed method uses the slice time window to find a normal template. During a time interval, the other network information is collected and then the distance of the collected information with the primarily collected data is computed. The loop of calculating a new distance is performed until the distance is less than the threshold. The first usual pattern is the data collected between the initial time and the start of the present slice window. Then in the anomaly detection technique, the data which is inconsistent with the normal profile is detected as an intrusion. Theoretical analysis is used to evaluate the proposed method. Collected data in the evaluation of the proposed method are derived from the measurements of the Intel project. The responsibility of the network is to record temperature, humidity, light, and voltage within a time interval of 30 s. The employed data includes about 2.3 million data collected from these sensors. Fewer resource requirements, which make it more appropriate for the perception layer of IoT, self-adaptive, low false alarm, and low communication overhead are advantages of the method. However, all anomalies cannot be detected.

Moreover, a game model has been declared by Ding et al. [75]. It enables the nodes for receiving the optimal amount of network resource to use in information security. In contrary to the selfish nodes, which tries to send packets to a destination with the optimal amount of resources, the malicious nodes try to advertise false routing information, therefore, they use a lot of resources. In the proposed method, the nodes activity among the selfish and attacker has also been monitored. In this method, a feedback solution that lets each node to pick up the optimal amount of network resource is used. The nodes use these resources in packet

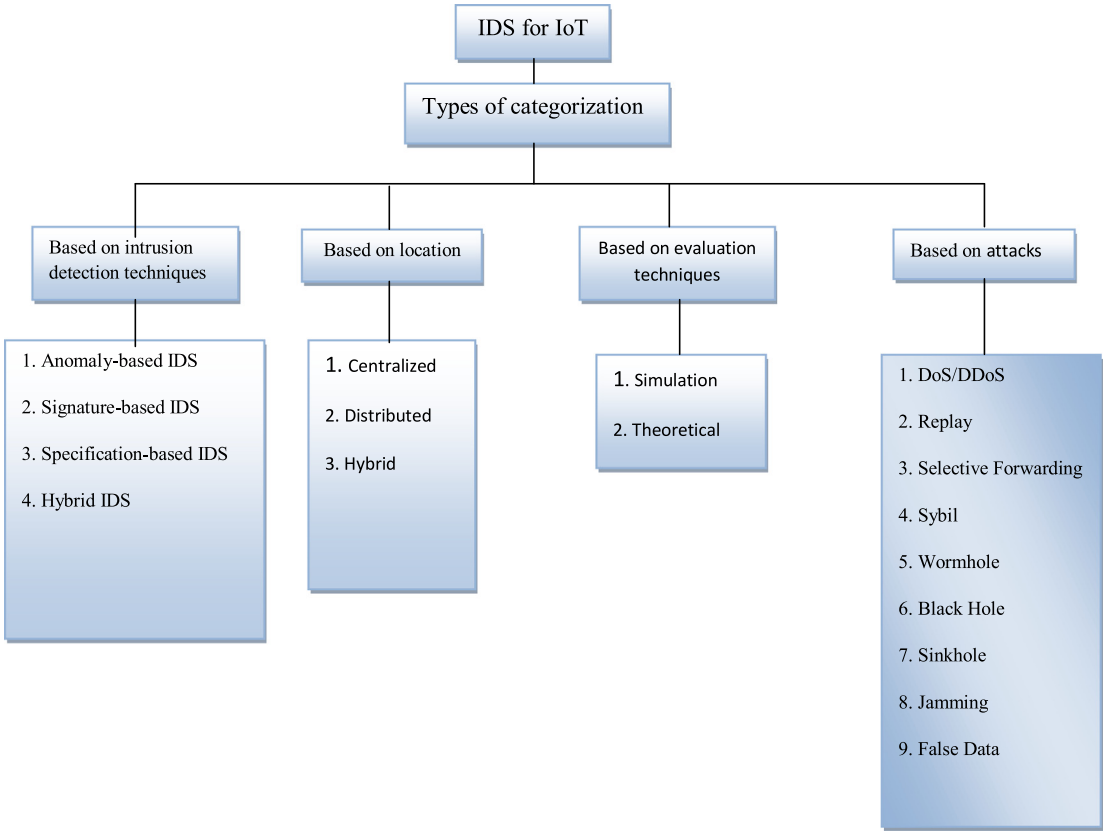

Fig. 7. IDS for IoT; categorizations based on intrusion detection techniques, the location of IDS, evaluation techniques, and type of attacks.

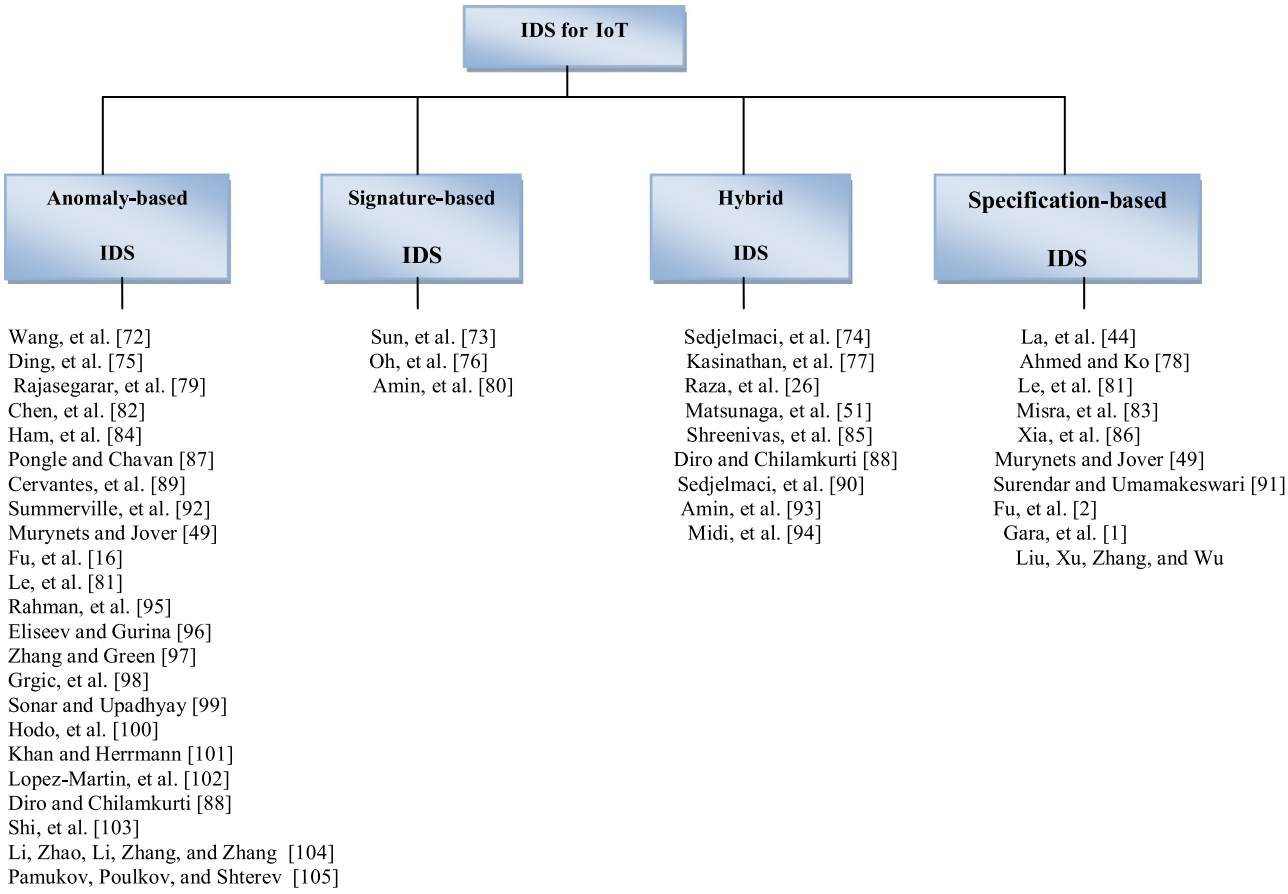

Fig. 8. IDS for IoT; categorization based on intrusion detection techniques.

forwarding, then monitor the effectiveness of the resources against the vulnerability to some attacks. Four key difficulties of stochastic diversion hypothesis keep its effective usage in the field of the IoT: (1) Stochastic game theory does not demonstrate energy to model games with lots of players. (2) The existence of a large number of moves states in the IoT networks causes come difficulty to study the dynamic behavior of the network. (3) In stochastic game theory frameworks, models are produced for all situations such as numerous inconsequential situations. The proposed framework models a subset of situations, which are imperative to official choices so that accessible assets are successfully used. (4) In the IoT, an arrangement of needs ought to be utilized for all gadgets when it is impractical to give distinctive needs to each player by utilizing stochastic game theory. A numerical example is used to evaluate the efficiency of the proposed method. In the evaluation, two teams of self-help and malicious nodes are used. In the experiment, the number of nodes is 1000 and the number of malicious nodes is 200. High detection accuracy, good performance, and low resource consumption are the advantages of the proposed method. The important disadvantages of the method are that it has a low combination with the IoT and it is not real-time intrusion detection.

Rajasegarar et al. [79] have proposed a distributed anomaly detection architecture which utilizes numerous hyper ellipsoidal groups to show the information at every node and detect the global and neighborhood abnormal behavior in the system. Specifically, a score is given to each hyper ellipsoidal model in the anomaly scoring technique by calculating the distance of the ellipsoid with their neighbors. The nodes in the network collect the data measurements and distinguish the local and global abnormal activity. When a sensor node collects the data from the network, it can determine the anomalies based on collected data of nodes. The measurements of local anomalies collected from several sensor nodes in the network are united to determine the global anomalies. The numerical and theoretical methods with real datasets are used to evaluate the method. In order to evaluate the efficiency of the method, two sets of experiments have been used. Initially, real-world datasets of WSNs namely HI, GSB and REDUCE have been used to evaluate the performance of the method. In the second step, the efficiency of the distributed method with the centralized method and the other presented methods in the article are compared using the mentioned datasets. According to the evaluations, it is concluded that the distributed method has a significant detection accuracy compared to the centralized method and at the same time significantly reduces the communication overhead. Some merits such as communication overhead, detection accuracy, communication complexity, a lifetime of the network, and detection rate are improved in the scheme. The disadvantages of the method are that it is not real-time intrusion detection and low detection rate increases by the width of ellipsoidal.

Also, Chen et al. [82] have demonstrated a fusion-based protection component to decrease the harm brought by deliberate attacks. By detailing the attack and IDS procedure as a zero-sum game, the result of the game is utilized to assess the adequacy of the method. It is assumed that all of the nodes have the same anomaly-based IDS which used the Neyman Pearson standard. In order to reduce the number of intrusions, each node sends one-bit information to the fusion center. Theoretical analysis is used to evaluate the proposed method. The proposed method provides the optimal attack/defense strategies for the attacker and defender. It

Table 6
A side-by-side comparison of the selected anomaly-based IDS techniques.

Paper	Main idea	Advantages	Disadvantages
Fu, et al. [16]	Detecting anomalies with the hierarchical distributed scheme.	• Self-adaptive • Low false alarm rate • High detection accuracy in theory • Low resource consumption	• All anomalies not triggered by malicious IDS • High delay
Ding, et al. [75]	Providing network security with a non-cooperative differential game model with using feedback Nash solution.	• High detection accuracy • Good performance • Low resource consumption	• Low combination with IoT
Rajasegarar, et al. [79]	Detecting anomalies for hyper ellipsoidal clusters along with an anomaly detection algorithm.	• Low communication overhead • High detection accuracy • Low communication complexity • An improved lifetime of the network • High detection rate with a smaller width of ellipsoidal	• Low detection rate with increasing of the ellipsoidal
Chen, et al. [82]	Decreasing the damage caused by attacks with a fusion-based defense mechanism.	• Enhanced robustness • Low communication overhead • Low computation complexity Can be implemented in real-time	• Complex security mechanism • Excessive energy consumption • Low performance • Supportably specific attacks • Attacker informed about network topology
Ham, et al. [84]	Detecting Android malware with a linear SVM	• High true positive rate • High detection accuracy • Low false alarm rate • High precision	• High time overhead • Heavy implementation
Wang, et al. [72]	Online training and detecting mechanism for large-scale IoT services.	• Real-time intrusion detection • Improved system performance • Improved the lifetime of the network • Improved detection accuracy • Low computation overhead	• High energy consumption • Detecting a limited number of attacks
Pongle and Chavan [87]	Detecting of wormhole attacks with the location information of node and neighbor information	• High energy efficiency • Real-time intrusion detection • Low resource consumption • Low packet overhead	• Low detection accuracy • High false positive rate • Can detect only one type of attack
Cervantes, et al. [89]	Detecting sinkhole attacks with INTI	• High detection accuracy • Low false positive rate • Low false negative rate	• Can detect the only limited number of attacks • High computational overhead
Summerville, et al. [92]	Detecting normal and abnormal behavior by a lightweight scheme	• Lightweight implementation • High detection accuracy • Low false positive rate • Low latency • Highly configurable	• High computational overhead
Zhang and Green [97]	Detecting DDoS attacks with a lightweight IDS	• Lightweight	• High power supply • High computing resources • Long processing time
Eliseev and Gurina [96]	Detecting anomalous behavior of network server on the basis of the correlation functions of a request-response manner.	• Lightweight IDS • Consuming modest resources • Not require permanently updated parts	• High computational overhead • High delay
Rahman, et al. [95]	Detecting attacks with an NF-based scheme	• High reliability • High detection accuracy	• High computational overhead
Grgic, et al. [98]	Detecting the malicious node in the IPv6-based IoT with the adaptive distributed system	• High energy efficiency • Good detection accuracy • High adaptability • Tolerant of some node failures • Real-time intrusion detection • Minimal resource consumption	• High false positive rate

(*continued on next page*)

Table 6 (*continued*)

Sonar and Upadhyay [99]	Detecting DDoS attacks by an agent-based method using of BlackList and GreyList.	• Low false positive rate for the small number of attacks • High true positive rate for the small number of attacks • High detection accuracy for a small number of attacks	• It is not real-time • Not suitable for a large number of users • High false positive rate for large number of attacks • Low true positive rate for a large number of attacks • Low detection accuracy for a large number of attacks
Hodo, et al. [100]	Detecting DoS attacks with three layers ANN which uses the MLP with supervised learning.	• Running expert system to build knowledge-based system features • Optimization of real-time usage • Efficient on incomplete data sources • Identifying known suspicious events. • High detection accuracy • Low false positive rate • High true positive rate	• Based on a probability estimation. • Needing more time for good efficiency
Khan and Herrmann [101]	Detecting attacks using three algorithms based on a trust management mechanism that allows devices to manage reputation information about their neighbors.	• High energy efficiency • Flexibility • Easily accommodated to other types of attacks • High detection accuracy • Least amount of network load • Real-time • Low resource consumption	• High false positive rate • High communication cost
Lopez-Martin, et al. [102]	Proposing an Intrusion Detection Conditional Variational Auto-Encoder (ID-CVAE) method based on a specific architecture	• Low complexity • Low computation latency • High detection accuracy • Low latency	• High false positive rate • Training stage use many resources
Diro and Chilamkurti [88]	Detecting attacks in social IoT with a deep learning approach	• High detection accuracy • Real-time • Low false alarm rate	• High training time • Training use many resources
Shi, et al. [103]	Detecting attacks with immunity based IDS.	• Adaptability • Self-learning • Robustness • Real-time • High detection accuracy	• High resource consumption • High false positive rate
Li, Zhao, Li, Zhang, and Zhang [104]	Detecting attacks with AI-based two-stage IDS which is improved by Software Defined Network (SDN)	• High accuracy • Low overhead • Low false alarm rate • Low processing time	• Not implemented in the real word
Pamukov, Poulkov, and Shterev [105]	Detecting attacks with NSA classification algorithm for creating a training set and a NN is trained to do the actual classification	• High detection accuracy • High scalability • Low false positive rates	• It is not real-time IDS

also ensures that no player's payoff increases with one-way strategy, so the game output will be a robust and reliable amount for performance evaluation. In fact, the critical factor in network failure can be done by conducting empirical experiments on data collected on the network or using complex network theory to identify the characteristics of the network. To compare and evaluate the efficiency of the method, the synthetic network models and collected parameters are used from real-world datasets. The proposed fusion-based component is online IDS, enhances the robustness, offers low communication overhead, and decreases computation complexity. However, the node degree is not the best centrality measure for minimizing the biggest segment estimate. Further, the attacker is able to damage all nodes of the network because it is informed about the network topology. Furthermore, the paper only focuses on mitigating impacts of specified intrusions.

Ham et al. [84] have proposed a linear Support Vector Machine (SVM) to distinguish intrusions on Android for the IoT services. The strategy is an Android malware-detection component utilizing machine learning calculations. In the proposed method, it is possible to detect the attacker by reviewing the data collected through resource monitoring. In the proposed method, the resources in an Android environment have been audited and malware behavior is detected based on the collected data. Accordingly, behavior-based detection has been used to enable automated anomaly classification and ensure the detection accuracy using a machine learning method. The behavior-based detection utilizes a machine learning technique to empower mechanized malware arrangement and guarantee its recognizable proof and exactness. In order to evaluate the proposed method via theoretical analysis, 14 normal and 14 malicious nodes which embedded with malware are used. The dataset includes 90% normal application and 10% malicious application. The reason for dataset combinations is that the normal applications are more common than malicious applications when examining the percentage of applications used in real portable space. Evaluation results have shown that the SVM-based malware detection in the IoT has high detection accuracy, high true positive rate and low false positive rate of detection in comparison with other machine learning techniques. However, it is not a real-time IDS and it has timing overhead. Further, it suffers from heavy implementation overheads.

Wang et al. [72] have configured an online anomaly training and detection method for IoT, which is used the reversible-jump Markov Chain Monte Carlo (MCMC) learning. Training of dependency structures is performed by integration of node status data and an integrated probabilistic model. Next, the anomaly tree structure is organized. Also, the parents with a normal presentation and distribution are sampled by reversible-jump MCMC. MATLAB simulation environment has been used for simulation and assessment of the system. In order to evaluate the efficiency of the proposed method, collected data of actual laboratory in Beijing's smart city environment has been used. The collected measurements at a base station are investigated every 5 or 30 days. The dataset is of medium size consisting of slightly more than 50,000 samples. The outcomes of the evaluation have shown the technique exactness in the prediction of the flow system and administration structures from manufacturing information. Real-time intrusion detection, system performance improvement, lifetime enhancement, accuracy improvement, low computation overhead, and better use of available resources are the advantages of this method. However, it has some demerits such as high energy consumption and detecting a limited number of attacks.

Furthermore, Pongle and Chavan [87] have proposed an IDS for IoT, which is equipped for recognizing the wormhole attack. The proposed technique utilizes the local data of the node and neighbor data to recognize the intrusion and get flag quality to distinguish malicious nodes. Neighbor information from all sensor nodes is collected and has been stored. Then the verification of the stored information using the distance between the node and that neighbor is performed. Network nodes detect the changes in the neighbor nodes and send their information to centralized modules in the border router. Then the centralized modules store and analyze this data to detect intrusions. The Cooja simulator is used to evaluate the method. The Tmote Sky nodes are also used in the simulation. Generally, it is thought that a 6BR is not a constrained node, so it can be a personal computer, a laptop; however, there is no PC equivalent 802.15.4 devices, therefore, the 6BR natively run on Java native interface on Linux. Radio interface cc2420 is used as the protocol configuration. At the network layer, IPv6 over Low-Power Wireless Personal Area Networks (6LowPAN), IPv6 and Routing Protocol for Low-Power and Lossy networks (RPL) as routing protocol are used. A User Datagram Protocol (UDP) is also used as a transport layer protocol. The memory utilization is less in comparison with aggregate accessible sizes. Energy consumption, packet overhead, and memory consumption are the upsides of the method and high false positive rate, low detection accuracy, and detection of only one type of attacks are considered as its demerits.

In addition, Summerville et al. [92] have mentioned an ultra-lightweight deep packet anomaly detection scheme to run on resource-constrained IoT devices for identifying normal and abnormal behaviors. The identification function is executed as a lookup table, letting both fast assessment and flexible feature space exhibition. Bit-patterns provide flexibility to match between a bit-pattern and n-gram sequences for payload modeling. This efficient and simplistic detector allows the representation of arbitrary discrete shapes in the feature space, which provides an ability to distinguish anomalous payloads from normal ones. By employing a direct representation of the feature space for the discrimination function, the detector can make a fast packet classification decision. The approach can be deployed on the IoT or can be built into network appliances and firewalls. The affectivity and ability of the detectors for identifying anomaly packets from a huge amount of attacks and device-specific traffics is high. Theoretical analysis is used to assess the proposed method. The evaluation of the method is done with the traffic obtained from two Internet-enabled devices: an interactive networked video camera and a weather station. Since the IoT will bridge the cyber and physical worlds, these two types of devices are a good starting point for analysis. The traffic has been collected from two IoT devices, as well as generic Hypertext Transfer Protocol (HTTP) traffic, to obtain three benchmark datasets: IoT control device, IoT sensor device, and generic HTTP.

Also, Zhang and Green [97] have demonstrated a lightweight IDS using learning automata for distributed denial of service attack over the IoT. An attacker behavior can be distinguished from an ordinary user by its high frequency of sending requests and the same content of the sent packets. An attacking node is always sending the same request with certain higher frequency. Learning automata is a strategy which intelligently determines the packet sampling rate from the environment to prevent the DDoS attack. The learning automata mechanism takes a set of sampling rates from the random environment as an input and responses a best-suited action according to the given actions as an output. A preset maximum servicing capacity for each layer will be used as a threshold value for issuing a DDoS alert among the neighboring nodes once it is exceeded. Theoretically, in the sub-network, there is only one chance to be served and blocked the serving node for each attacking node. Once it has been detected as an attacker, its packets are to be rejected and dropped. So, with the implementation of the defense mechanism in the working and monitoring nodes, the effect of a DDoS attack will be relieved within one service cycle. The Cooja simulator is used to evaluate the method. Low latency and lightweight implementation are merits of the

proposed method and high power supply, high computing resources, and longtime processing are demerits of it.

Furthermore, Cervantes et al. [89] have suggested a sinkhole attacks detection method on IPv6 over 6LoWPAN within the routing service of the IoT. Watchdog reputation and trust methodologies with dynamic clustering are integrated in order to analyze the behavior of devices. Cluster configuration module describes a header-based hierarchy establishing node clustering, which classifies them as members. Nodes are responsible for forwarding messages, monitoring module count, and the amount of output, and input messages. If the numbers of input and output messages are equal, then that node behavior is normal, otherwise, there is an anomaly in the node behavior. The Cooja simulator is employed to assess the method. The proposed method has been evaluated and compared with SVELTE (means elegantly slim) in terms of detecting sinkhole attacks. The simulation environment consists of a real urban street where there are different types of things. The simulation consists of 50 nodes, some of which are fixed and some are mobile that indicates the average of users crossing the street. Users have wireless devices, including cell phones, PDAs, laptops, and they are in an enclosed area. Things in the street move with speed between 0 m/s and 6.94 m/s. The number of malicious nodes is between 10 and 15. This value is about 20–30% of the total system nodes. The simulation environment is carried out in the dimensions 100 * 100 m and 80 * 80 m. The simulation time is the 1500 s. The method has some upsides such as high detection accuracy, low false negative rate, and low false positive rate. However, it can detect only one type of attack.

Rahman et al. [95] have presented Neuro-Fuzzy (NF)-based IDS to identify the incidence of Physical (PHY) and Medium Access Control (MAC) layer intrusions in the IoT where an IDS uses the Artificial NF Interface System (ANFIS). The ANFIS receives some data as input and generates IoT intrusion detection as a result. The method monitors the activity of the network and then collects the data. The data in the database are updated in a dynamic way. The proposed method contains some steps such as network behavior analysis step, feature identification and selection step, and feature extraction with a classification step. The algorithm which is proposed by the method receives network activity data as an input and shows the possibility of an attack occurring as an outlet in the IoT. MATLAB simulator is used to simulate and evaluate the proposed method. Three main parameters including transmitted packets received packets, and packet loads are used for simulation. The transmitted and received packets are considered as inputs of the ANFIS and the packet loads as its output. The entire dataset is divided into testing and training datasets which are used for NF learning. Data that are used against DoS attack detection are captured from the center for applied data analysis. The proposed method provides high reliability in the security of IoT environment. It also has high detection accuracy.

Moreover, Eliseev and Gurina [96] have proposed an approach to detect anomalous behavior of the network server on the basis of the correlation functions of a request-response manner. Two algorithms are demonstrated, the first one is based on the Pearson correlation coefficient and another is based on neural network classifier. Two algorithms employ opposite approaches to the detection of anomalies on the basis of the correlation functions of the server response to requests. The properties of the algorithms are studied on real server traffic. In the first algorithm, an averaging of the correlation function is done and it is assumed that the similarity of the current correlation response to the average is a sign of the norm. The second algorithm is based on associative memory and neural network. It allows remembering and recognizing many normal forms of correlation function without explicit averaging. Close to zero reconstruction error which is offered by a current correlation function is recognized as a normal one. It seems that the first algorithm is only suitable for a relatively simple server with a simple scenario of regular interaction. Nevertheless, a specific device is designed for use in industrial automation systems and the IoT may be a viable option given the efficiency of implementation. The second algorithm has a much greater potential for devices with complex communication protocols and is also applicable for network servers using standard application-level engines. Both algorithms can be used as embedded lightweight IDS in the area of Machine to Machine (M2M) and the IoT. MATLAB simulator is used to simulate and evaluate the proposed method. The program of installing both algorithms involves collecting network traffic as much as possible in different scenarios and server loads. It takes a lot of time for network servers throughout the working operation. For example, the total time spent for monitoring server traffic data, which is essential for the method, takes about 3 weeks. Data can be used to set up the algorithm of anomaly detection in the entire part of the devices and placed in the firmware of all devices. It is a lightweight IDS, consumes low resources and does not require permanently updating. However, the setup procedure for both algorithms contains the collection of network traffic as possible in many scenarios and server load. Also, during the working process, the whole process can take reasonably a long time.

Also, Grgic et al. [98] have demonstrated a system for detecting malicious nodes in an IPv6-based WSN (being the basis of the IoT). In the proposed system, all IDS modules listen to their neighbor's traffic and collect data that represent input parameters into the collective decision-making process. Then the maximal numbers of allowed packet drops are defined as a threshold. If dropped packets deviate the threshold, the observed node is considered as suspicious. The proposed security framework provides basic security premises, including authenticity, reliability, integrity, and availability. The proposed framework assesses the anomaly probabilities for suspicious nodes, where most existing IDS do not evaluate the damage level. Another preferred standpoint of the proposed framework is its flexibility for various application necessities accomplished by the adaptable (adjustable) malevolence threshold. The system for malicious node detection in the IPv6-based WSN is a fully distributed system, based on collaborative algorithms without relying on central infrastructure. IDS modules (agents) are implemented on every node in the WSN. The main task of the IDS agent is to monitor neighboring nodes (within the transceiver range) and to participate in the collective decision process. The system is fully adapted for the protocol stack in the IPv6-based WSN. The Cooja simulator is used to evaluate the method. The analysis of the proposed IDS is performed through 9 different scenarios in three different networks (6 nodes, 10 nodes, and 17 nodes). The first testing network includes 6 nodes (5 sensor nodes and the base station). Node 1 is the base station, while the others (2–6) are regular sensor nodes. A radio transceiver range is set to 30 m (circular area), while the interference area radius is 50 m. These values directly influence network topology and the establishment of the routes to the base station, since the possibility of direct communication between nodes depends on their transceiver range. After network initialization, each network node periodically (once a minute) sends its sensor readings to the base station (temperature, humidity, and illumination). Three scenarios with a different Rx/Tx success ratio are analyzed. This ratio is 100%, 80%, and 60%, in the first, second, and third scenario, respectively. All tests are performed with and without the IDS to draw a conclusion about the IDS impact on network performance. Good detection accuracy, high adaptability, tolerant of some node failures, real-time ability, and minimal resource consumption are the advantages of the method and high false positive rate is considered as its drawbacks. Also, the differentiating between misbehavior and malicious nodes is difficult, therefore, the anomaly-based IDS usually has a high false alarm rate. Further, because of analyzing a great amount of data, the delay is high.

Sonar and Upadhyay [99] have demonstrated an agent-based method to detect DDoS attacks on IoT and continue the activity of the system. The agents are software-based managers located between network and gateway or border router. It can detect the attack by taking a suitable operation to activate the network under such situation. Also, GreyList and BlackList as the special access control lists to give temporary or permanent access are employed. First, the learning period of the algorithm is started with running in normal traffic. Then it calculates the threshold values. The first time which an attack is detected, the IP pushes to GrayList. If the attack is detected from the same IP, again it pushes to BlackList. The proposed strategy is simulated via Cooja simulator. The learning time in the simulation is performed in the first 20 s to calculate the threshold values. The simulation of the attack begins for the next 20 s and is performed with another 20 s to check the system recovery. The simulation time is the 60 s and the number of normal clients are 5, 15, and 30. The number of attacking nodes is 5,15, and 30 and the RPL and UDP have been used as routing protocols. Low false positive rate, high true positive rate and high detection accuracy for a small number of attacks are considered as the advantages of the proposed method. However, it is not a real-time method and is not suitable for a large number of attacks.

Hodo et al. [100] have demonstrated an Artificial Neural Network (ANN) to detect DDoS attacks. The neurons of the ANN are used to form complex hypotheses, and then it evaluates them by setting the input nodes in a feedback process. In supervised learning, the neural network is used with a labeled training set, which learns a mapping from inputs to outputs and gives a labeled set of input-output pairs. The multilayer perceptron as a type of ANN is used in the proposed algorithm which is trained with a supervised algorithm with three layers. The network has a unipolar sigmoid transfer function in each layers' neurons and is trained with feed-forward and backward training algorithm for classification of the normal and abnormal behaviors. In order to evaluate the performance of the proposed method, the network with 2313 samples is trained where 496 samples are verified. The network under investigation consists of 5 sensor nodes. Four of the nodes are operating as clients and one as servers for analytical purposes. Traffic is received without modification with live traffic. The server node receives the information sent by the sensor nodes and answers them with data based on the received data. A single host is responsible for DoS attacks that send about 10 million packets. The sent packets during the DoS/DDoS attacks of the UDP are made by a custom C-based script. Running expert system to build knowledge-based system features, optimization of real-time usage, efficiency on incomplete data sources, identifying known suspicious events, high detection accuracy, low false positive rate, and high true positive rate are upsides of the method. However, it is based on a probability estimation and more time is needed for good efficiency.

Khan and Herrmann [101] have designed and evaluated three IDS mechanisms for IoT. The proposed mechanism uses a trust management model and allows devices to utilize the reputation information about their neighbors. In the Neighbor Based Trust Dissemination (NBTD), trust is implemented in a centralized manner. The border router calculates trust values periodically using the trust inputs received from the nodes in the Destination-Oriented Directed Acyclic Graph (DODAG). Thus, it is the only manager of reputation ratings for all the nodes in the DODAG. Also, Clustered Neighbor Based Trust Dissemination (CNTD) is used as a distributed approach to assess the trust values from the network. It assumes that the DODAG is segmented into several clusters that all of them have a cluster-head. The cluster-head gathers and calculates the reputation of each node in its cluster. It receives the trust values from the other nodes in the cluster periodically and aggregates them with its own trust values. If the variable of a reputation value exceeds a threshold, the node will be blocked and the border router is notified. Furthermore, Tree-based Trust Dissemination (TTD) uses the same topology as CNTD, but it reduces the surveillance of nodes. A node only supervises its parents to save network overhead. In consequence, the leaf nodes of a DODAG will not be monitored since they have no children. The proposed method is evaluated with MATLAB. The simulation scenario consists of 1000 nodes distributed randomly in a square environment of 100 * 100 m. For both algorithms, the system is divided into nine identical clusters. There are two different simulations to compare the results of the algorithms. In the first set of simulations, a number of different nodes are introduced to examine the impact of malicious nodes on the network. In the second set of simulations, different simulations are performed, in which an attacker is removed in a certain round. In addition, in both sets, the effect of algorithms on total network load is investigated. In the simulation, the malicious node is supposed to send misleading trust values randomly to its neighbors for ruining the IDS. High energy efficiency, flexibility, easily accommodated to other types of attacks, high detection accuracy, least amount of network load, real-time and low resource consumption are upsides of the method and high false positive rate and high communication cost are the downsides of it.

Furthermore, Lopez-Martin et al. [102] have proposed Intrusion Detection Conditional Variational Auto-Encoder (ID-CVAE) based on an infrastructure which inserts the attack labels inside the decoder layers. An anomaly-based supervised machine learning approach has been proposed which uses a deviation-based method to allow classifying a particular traffic sample with the attack label. The intrusion features are not used as a single input instead of it the attack features and the attack class labels are two inputs of IDS as it is done based on a Variational Auto-Encoder (VAE). To create a category with the VAE, there needs to have a large number of models where each model needs a particular learning module. Each learning module uses only the particular samples that are associated with the label being learned. ID-CVAE establishes a single model with a learning module that uses all learning data regardless of related labels. Theoretical analysis is used to evaluate the proposed method. The results are obtained using ID-CVAE and some other machine learning algorithms over NSL-KDD dataset. Low complexity, low computation latency, high detection accuracy, and low latency are the merits of the method and high false positive rate and using many resources in training stage are the demerits of the method.

Diro and Chilamkurti [88] have proposed a deep learning-based method to detect the attacks in social IoT. The human brain has the ability to learn from experiences and deep learning has also benefited from this feature of the brain. In addition, the brain has the ability to process raw data that has reached from the nerves. Deep learning also utilizes the ability of the brain to send row data to deep neural networks to classify them according to their training. Since fog nodes are closer to the smart infrastructure of social IoT, they are used to educate and maintain IDSs at the edge of distributed fog networks. The proposed method is a centralized method and can extend to the distributed system. Theoretical analysis is used to evaluate the proposed method. In the performance evaluation, the proposed method is evaluated over NSL-KDD dataset available in the CSV format. The dataset includes 125,973 training records, 22,544 records for testing, and 41 features. Before the training phase of the network, the existing features are encoded into discrete features that include 123 input forms and one label. High detection accuracy, online and low false positive rate are the upsides of the method and high training time and several resources usage in training are downsides of it.

Shi et al. [103] have demonstrated an Immunity-based IoT Environment Security Situation Awareness (IIESSA) system to effectively perform attack defense in the IoT environment. In IIESSA, the 6LoWPAN of IoT connects directly to the traditional Internet by

6LBR. The 6LoWPAN contains RouTer (RT), Security Awareness Center (SAC), and Security Sensor (SS), where SS presents all types of IoT devices. SS can communicate with other nodes of IoT by 6LBR or RT. It is an immunity-based security sensor in the IoT environment which contains extracting security elements module, evaluates security condition module which is responsible for adopting an artificial immune system to attack recognizing, forecasts the security situations of devices/nodes in the IoT and predicts security situation which is responsible for auditing the IoT environment. Using the immune vaccine system, SAC and SS can distribute new features extracted from network attack activities to the IoT using the vaccine distribution system, so, the security of IoT objects can be improved over time. The simulation platform of the proposed method includes the Cooja simulation software that runs on an operating system and personal computers, laptops, and resource-based devices. The attacks that are used in the simulation include Spoof, Sinkhole, and Sybil, etc. Furthermore, the network services provided on the IoT networks are essentially related to WWW, FTP, and E-mail. For the length of antigen and antibody, a 288-bit binary string is defined that includes source/destination IP address, source/destination port, protocol type, and so on. IIESSA has some upsides, such as self-learning, strong, compatibility and online. However, high resource consumption and high false positive rate are downsides of the method.

Pamukov et al. [105] have suggested a classification algorithm which is designed for IoT IDSs. The offered solution includes two distinct layers. First, a Negative Selection Algorithm (NSA) for creating a training set via the normal network behavior's knowledge. According to this data, a simple Neural Network (NN) is trained to do the actual classification. This multilayer method can remove the training complexity from the computationally and power constrained IoT devices. The layered structure of the algorithm provides the remotely performing of the training phase. Additionally, the negative selection layer lets training an NN only based on the self/normal behavior of the network. This algorithm called Negative Selection Neural Network (NSNN). Because of using NSA, the proposed approach can properly be classifying previously unobserved intrusions. The NSA is also employed for learning the "self" and creating a "non-self" set of data. Then those two sets used to train an NN, which performs the self/non-self classification. The NSA algorithm also employs the R-Continuous Bit Matching (RCBM) rule as a classification function. There is a "match" between two strings when at least n continuous bits are similar. The Number Negative Detectors (NDD*)* is also used to tell the algorithm how many "non-self" strings must be produced. The Negative Detector Set (NDS*)* includes the set of "non-self" generated by the NSA for an NN part by employing a single layer feed forward NN. The gradient descent learning delta rule is employed for training the NN. All simulations are carried out in MATLAB R2015a. Training and testing the algorithm are done based on KDD NSL dataset. Every sample in KDD dataset has 41 different features. The basic traffic features have been used since they provide most the meaningful information. The method has high detection accuracy and can detect close up to 100% (0.99 PPV against 90% AAT) of all unknown attacks. The algorithm is not an online method. Due to its scalability and immune holes issues, the NSA is obviously unsuitable for solving large-scale self/non-self classification problems.

Li et al. [104] have proposed an AI-based two-stage IDS which is improved by Software Defined Network (SDN). In the first phase, the Binary Bat Algorithm (BBA) with swarm division and binary differential mutation is used to select typical features. For the feature selection process, BBA is employed which includes iterations of position moving and target searching. The fitness function will be the evaluation metrics of the classifier after it has been qualified with the selected features. Also, SDN captures network packets and collects status information via centralized control. The controllers divide network packets into flows and bring them to the upper layer. Next, the controllers manage resources and organize specific actions for defending from attacks based on the classification results. Furthermore, BBA solves feature selection problems with high performance and acts better than traditional algorithms with a simpler structure, fewer parameters, and stronger robustness. Therefore, in the first stage, BBA improves its ability for searching optimal features. For evaluation, KDD Cup 1999 dataset has been used. Evaluation results have validated the optimality of the proposed algorithms in achieving high accuracy and low overhead. The results have also shown that the proposed IDS can improve the detection ability without much time consumption compared to existing solutions. The disadvantage of the method is that it is not implemented and evaluated in real-world scenarios. Table 6 provides a side-by-side comparison of the selected anomaly-based IDS techniques (Table 7).

5.2. Signature-based IDS in the IoT

To protect against various attacks, signature-based detection scheme plays an important role in taking up a great place after decades of development in both industrial and academic research. It uses the theory that the signatures of the various attacks generally are unchangeable and since the number of the malicious patterns is limited, it can be detected at the earliest stage [106]. Signature-based detections match the current behavior of the network against pre-defined attack patterns. In the IoT, signatures are determined first and kept on the device and each signature matches a certain attack. Commonly signature-based methods are easy to use, which needs a signature for each attack [26]. The remainder of this part is the survey of the chosen papers in this field.

Amin et al. [80] have demonstrated a mechanism with dynamic coding for implementing distributed signature-based IDS in IP-USN (IP-based Ubiquitous Sensor Network). In the method, first, signatures with various lengths send to their relative bloom filters. The output of the bloom filters is a bit array of the signature codes. After sending the content of arriving packets to the bloom filters, a pattern checking is performed and if a match is found, sensor node stops the processing of the packet and sends an alarm signal with signature-code to the sink for confirming the bloom filter match. To evaluate the efficiency of the proposed method, Snort signature-set is used. Snort can be considered as Defacto IDS for traditional IP networks. Snort version 2.8 has 13,339 signature strings. With a limited set of current programs for IP-USN, this collection signature can easily be considered as the upper limit for the number of signatures in the IP-USN. Low false alarm rate, high detection accuracy, low memory consumption, low energy consumption, and the lightweight nature of the system are the upsides of the proposed method. However, it is not a real-time IDS and it has unnecessary network transmission. Signature-based detection techniques use large memory because of maintaining signatures of the attacks. Further, these types of IDSs can detect a limited number of attacks.

Oh et al. [76] have proposed a security mechanism that uses a pattern-matching engine for the malicious nodes in the IoT. In resource-constrained devices, limitations of computation power and memory cause performance reduction. Then two strategies such as auxiliary shifting and early decision are defined in the paper. These techniques effectively decrease match operations in the IoT environment. In the patterns with the equal prefix values, character matching performs and the obtained information is used for recognizing the early termination of matching operation. The outcomes have demonstrated that the technique improves performance, especially when the quantities of examples turn out to be huge. To evaluate the proposed IDS for the IoT devices, a Raspberry Pi and the Omnivision 5647 sensor are used. The micro-controller of this device consists of an ARM1176 700 MHz processor, 256 MB

Table 7
A side-by-side comparison of the selected signature-based IDS techniques.

Reference	Main idea	Advantages	Disadvantages
Amin et al. [80]	Detecting network intrusions with a design of an IDS for IP-USN	• Low false alarm rate • High detection accuracy • Low memory consumption • Low energy consumption • Lightweight	• Unnecessary network transmission • Can detect a low number of intrusions
Oh et al. [76]	Detecting malicious nodes with the pattern-matching engine.	• Low computational complexity • Maximum speed up • Low memory usage • High detection accuracy for predefined signatures • High level of scalability	• Can detect a low number of intrusions • It is not real-time
Sun et al. [73]	Detecting the malicious attacks by the cloud-based anti-malware system for the IoT called CloudEyes	• Efficient security service • Trusted security service • High data privacy • Low-cost communication • Low time consumption • High detection accuracy for predefined signatures	• High memory consumption • Can detect the limited number of attacks • High false positive rate

of synchronous dynamic random-access memory and 2 GB flash memory. The algorithm can contribute to an abnormal state of adaptability to pervasive numerous pattern-matching algorithms. In any case, it can recognize the predetermined number of attacks and just the attacks from predefined signatures can be detected. In the patterns with the equal prefix values, character matching performs and the obtained information is used for recognizing the early termination of matching operation. Also, it has low memory consumption. However, the method can detect low numbers of attacks.

Sun et al. [73] have proposed a cloud-based framework for intrusion detection called CloudEyes. In the client side, CloudEyes implements a lightweight scanning agent which uses the digest of signature fragments to dramatically decrease the range of accurate matching. CloudEyes uses a lightweight scanning operator and the digest of the signature fragments to lessen the range of accurate matching. The cloud server, with the implementation of the database, presents a summary of the signatures in the form of a reversible design. In other words, a summary design is produced that indicates the existence of the signatures. The cloud updates the signature database and designs periodically and sends the places in the sketch. The user for sending the file first divides the content of the file into segments based on the correspondence method with signatures, and the non-like parts are also sent with the latest digest. Suspicious Bucket Cross Filtering (SBCF) mechanism has been designed for the cloud to locate the malicious file segments based on sent segments from the client, which is suspicious. The C language is used for simulation and evaluation of CloudEyes. CloudEyes is implemented based on the ClamAV signature file and signature model with approximately 7 K lines of C/C++ code, with 4.5 K for the cloud server and the rest for the client. The CloudEyes cloud servers connect with each other through the socket transfer protocol. The assessment of the effectiveness of the method demonstrates that the proposed method has the ability to effectively defend against internal attacks, has low network traffic and low memory consumption. However, only the attacks from predefined signatures can be detected.

5.3. Specification-based IDS in the IoT

In this section, the specification-based IDSs have been overviewed. In the IoT, specification-based and anomaly-based IDSs are similar because both of them recognize intrusions when a deviation occurs from normal behavior. However, specification-based approaches do not rely on machine learning techniques. In these schemes, specifications are manually developed and captured legitimate system behaviors [107].

Misra et al. [83] have presented a Service Oriented Architecture (SOA) as a system model for the detection of attacks in the IoT environment using learning automata concepts. The SOA acts as a middleware which provides a platform for developing various applications for IoT. So, its amount varies with different layers and objects. In this step, the system detects the attack on any object in the IoT. The IDS uses a DDoS alert (DALERT) if the number of requests is greater than the defined value for each layer. DALERT is sent to all nearby neighbors of objects that will distribute this alert to other nodes. In nutshell, this phase identifies a DDoS attack and is carried out totally on the servicing device i.e. server. During this step, other objects maintain their normal performance. The proposed method indicates the possibility of attacks and cannot confirm an attack. The efficacy of the strategy is validated via the experiment results. The proposed method has been evaluated by simulating under the IoT conditions. The simulation platform for the proposed method consists of five objects. Object 1 is a thing that connected to the Internet which has the ability to provide the Internet for other things. Object 2 behaves as a simple bridge in the network, which has the task of sending other object requests to the serving objects. Object 2 does not request any service and it has a duty to send the requests. Objects 3, 4 and 5 are the basic devices to send the requests. Since Object 2 is the closest device to the rest, so, the rest of the objects send their request to it. For evaluation, the simulation time is 100 s. The attack rate of the object 3 is 50 and the attack rate of the object 4 is 33. The proposed system has low energy [108] and low computational power consumption. However, the approach strongly depends on the experience of the network administrator, which is a characteristic of the specification-based method. Also, wrong specifications may cause exceeding false positives and false negatives, therefore, a considerable risk to network security may occured.

Furthermore, Murynets and Jover [49] have proposed two methods for recognizing intrusions Short Messaging Service (SMS) activities and attacks on a combination of cluster and individual device levels in the IoT. After detecting attacks automatically, the method tries to determine the cause of the anomaly. The new

communication systems enable as part of IoT with the combination of the Internet and cellular M2M mobility networks. The algorithms are based on a volumetric and a contact-based analysis. The volumetric-based analysis is responsible for the detection of anomalies. When a deviation from the pre-defined pattern is detected, one can determine what device or cluster of devices generates the anomaly. The latter is responsible for tracking and analyzing the connections of each device. The combination of two methods can recognize all types of independent intrusions such as DoS attacks. Theoretical analysis is used to evaluate the proposed method. To evaluate the performance and of the proposed system, the network robustness is measured by solving linear programming problems with respect to the specified network. The proposed method provides an indirect defense/attack strategy for the attacker and defender, the game's equilibrium can eliminate the possibility of a player payoff with a change in strategy, and the output of the game's equilibrium is fixed. Also, the robustness of the network is measured and is used as an acceptable benchmark to evaluate the performance. It has a high detection accuracy. However, it is not a real-time IDS and has a complex implementation.

Xia et al. [86] have demonstrated a new routing protocol named Privacy-Aware routing protocol (PALXA). PALXA includes two processes: route setup and maintenance. In the routing setup, the most optimal path has been found. In the routing maintenance, PALXA uses the channel sensing strategy to realize the maintenance of the route path. In the specific routing maintenance process, the traffic of the predecessor node and the subsequent node is detected by each relay node. Also, the malicious behavior of the subsequent node is detected. Then the node will detect the results, compare them with the threshold values, and then determine whether the predecessor node and the subsequent node are in the presence of anomalous behavior. If the predecessor node and the successor node are judged as the malicious node, route preservation information is returned to the source node. The source node starts the path detection procedure and finds the most optimal path for sending the remaining packets after receiving the route preservation information. Finally, MATLAB simulator is used to perform experiments and performance analysis. Good detection accuracy and low latency are upsides of the methods. Also, the threshold value must be defined meticulously to prevent the positive rate and low detection accuracy.

Moreover, La et al. [44] have suggested a game theoretic model to examine the problem of deceptive attack and defense in a honeypot-enabled network in the IoT. The attackers use different types of attack which can be suspicious or looking normal activity to deceive the defender. Also, the defender can use honeypots as a tool to deceit the attacker. The system analyzes the incoming traffic using predefined rules, and if any object sends suspicious traffic, it will be sent to honeypot for further analysis. The rest of the traffic is sent to ordinary destinations. To prove the method, the MATLAB software has been used. Following multiple rounds of the game, the output is monitored and recorded. The method is flexible, has high detection accuracy and provides a real-time capability. However, high additional resources and converge time are disadvantages of the method.

Also, Ahmed and Ko [78] have proposed a method against the black hole attack, which includes a local decision and a global verification process. The information about the relations among the nodes is collected to detect a suspicious node in the local decision process. Every node observes the communication behaviors of its neighbors by overhearing data packets transmitted by its neighbors and attempts to identify a suspicious node based on their behaviors in the network. If the transmitted data packets of a node are greater than a given threshold value of its neighbor, the node identifies the neighbor as suspicious. Further, if a node determines that the upstream node of a suspicious node does not initiate responsive action, then the upstream node is also judged to be a suspicious node. When a suspicious node is identified, it undergoes a second process of further inspection of the neighbor. If the node is identified as a suspicious node, the second process initiates. For verification of the suspicious node, it initiates a query to determine if the root node receives the packet that the verification node could not overhear from the root. It then determines if the suspicious node is malicious depending on the query result. In order to evaluate the efficiency of the proposed model, simulations under different conditions and scenarios in the Contiki 2.7 operating system and Cooja simulator have been performed. The proposed method will be evaluated against standard RPL and RPL with attacker nodes. Each node has a communication range of 50 m and an interference range of 100 m. The network topology is such that it allows the connection of each node with a sink through several steps. The black hole nodes in the simulation environment start their attacks after the implementation of the initial graph. Each node sends its data packets to the sink at specified intervals. The simulation for each scenario has been performed 15 times and the average value for each metric is displayed. The evaluation results have demonstrated that the proposed method can increase the packet delivery rate and can detect a black hole attack. Also, the method has a high true positive rate. However, with increasing the percentage of infected nodes, the true positive rate, false positive rate, an end-to-end packet delivery delay, and the detection accuracy are decreased.

In addition, Le et al. [81] have proposed an RPL networks specification for checking the node behaviors. The proposed method consists of two steps. In the first step, the RPL protocol is simulated in normal conditions and a series of trace files are obtained. Therefore, all the conditions for the network topology are defined. The generated module has usability as a confirmation module for discovery. In the second phase, the knowledge of the RPL profile of the detection algorithms has been translated. Cooja simulator is employed to assess the proposed method. The simulation for testing the proposed method consists of 100 nodes which are randomly distributed in a square area of 60 $\times$ 60 m in which each node has a transmission range of 50 m. There is a sink in the center and 11 cluster heads cover the activity of 88 other nodes in the network. Each node sends packets to the sink every 60 s, and aggregated data is sent to the sink every 2 min. The specification-based module in the IDS is implemented in the cluster head to analyze the collected data. Simulation results have demonstrated that the proposed IDS has a high detection accuracy in distinguishing RPL topology attacks. High detection accuracy, high scalability in a large network and high energy efficiency are merits of the method. However, it suffers from high overhead and a long processing time.

Surendar and Umamakeswari [91] have proposed an Intrusion Detection and Response System (InDReS), which relies on constraint-based specification model to detect a sinkhole attack. Sensor nodes are grouped into a cluster and the maximum probability node becomes leader nodes and sends an announcement message to its adjacent nodes. The network is deployed with a set of observer nodes. These nodes perform the node monitoring process and identify the packet drop count of adjacent nodes. The observer nodes apply a ranking to each adjacent node. The output is compared with a threshold value to determine the malicious node isolates and reconstructs the network. The NS2 simulator is used to evaluate the method. The simulation is done in a 500 * 500 grid environment. The number of sensor nodes used in the simulation is 150. The number of the central station 10 and the number of observer nodes is 30. High packet delivery ratio, low packet drop ratio, low energy consumption, and low overhead are the advantages of the proposed method. However, it depends on expert admin, which is considered as its weakness.

Fu et al. [2] have analyzed the intrusion detection requirements of IoT environment and then have demonstrated an intrusion detection technique for the IoT networks based on an automata model. The method uses an extension of labeled transition systems to propose a uniform description of IoT systems for detecting the intrusions. The demonstrated automata-based IDS for IoT also consists of four major components: event monitor, event database, event analyzer, and response unit. The event monitor records the transmitting data into digital files and sends the files to the IDS event analyzer. Three databases are required in the event database: standard protocol library, abnormal action library, and normal action library. The IDS event analyzer includes three basic models: the network structure learning model, the action flows abstraction model and the intrusion detection model. The collected packet data need to be sent to network structure learning model first to make the IDS system receive a universal view of the network topologies. The collected online packets from IoT also should be sent to the action flows abstraction model. Through this model, the packets will be allocated according to the device features which are identified through the help of network structure learning model and the standard protocol library. In abnormal action, the library is employed to evaluate the results and in the second step, anomaly detection will be performed to identify the internal attack. In this step, a normal action library will be helped to identify the input transition sequence is normal. The response unit provides reports and alerts to IoT networks that there is intrusion risk. The Raspberry Pi 3 simulator is used to evaluate the method. The router is connected to a server, and the MySQL server is used to build the database tables. In this article, the port-mirroring is used on the router. The Wireshark is installed on the server side to collect packets sent from the IoT gateway. In the testing environment, the Remote Authentication Dial-In User Service (RADIUS) applications are used as services which are running on IoT networks. The RADIUS protocol is an application layer protocol which forwards data through UDP traffic. Therefore, when the Wireshark receives IP traffics, the RADIUS messages can be detected. The real-time feature, easy implementation, and low complexity are the upsides of the method and high resource consumption and low detection accuracy are downsides of the method.

Gara et al. [1] have focused on detecting selective forwarding attackers in IPv6-based mobile WSNs and IoT when the RPL is used. The method is an IDS that combines sequential probability ratio test with an adaptive threshold of acceptable probability of dropped packets. The proposed IDS is composed of two modules: a centralized one situated on the sink node and a distributed one situated on routing nodes. Each of the routing nodes collecting information from neighboring nodes and storing them in a table as the first step in the data gathering step. In data analysis step for each received hello packets, the sink computes the number and the probability of dropped packets. The sink node can verify for each time period that a node does not tell the correct number of packets. The decision step aims to detect malicious nodes and minimize the false positive and false negative rate. Finally, the sink encapsulates their corresponding identifiers in messages. If the sink node initiates a global repair in the network, messages will be sent. Each node received packets discards compromised nodes from its parent list. To evaluate the proposed method, the Cooja simulator is used. This simulator is based on the RPL protocol and has the ability to recognize the behavior of real nodes. High detection accuracy and high true positive rate are upsides of the method and high communication overhead, high latency, high resource consumption, and high false positive rates are the downsides of the method. Table 8 exhibits the side-by-side comparison of the selected specification-based IDS techniques.

Finally et al. [109] have proposed an IDS of the IoT by Suppressed Fuzzy Clustering (SFC) algorithm and Principal Component Analysis (PCA) algorithm. In this algorithm, the data are categorized into high-risk data and low-risk data. At the same time, the self-adjustment of the detection frequency is done according to the SFC and the PCA algorithm. PCA algorithm can decrease the number of variables and remove features with low discriminations. Because of the quickly increasing data transmission size in IoT, feature extraction can be extremely time-consuming. To assurance the good efficiency and effectiveness of IDS, extractions of feature vectors are obtained which were achieved by the PCA algorithm by traffic classification. In this way, the efficiency and effectiveness of IDS can be improved. The results have shown that compared to the traditional method, this method has better adaptability. High detection efficiency and low detection time are other advantages of the method.

5.4. Hybrid IDS in the IoT

In order to detect the usual behavior of a node, the anomaly-based IDS employs a training process to reach a high detection rate. High false positive rate and computation cost are downsides of the anomaly-based IDS and high storage cost and a limited number of attack detection are the downsides of the signature-based IDS. Then the hybrid scheme was suggested to deal with drawbacks of two methods. In the hybrid scheme, the signature-based scheme has been used to detect known attacks and anomaly detection scheme has been used when an unknown attack is detected [74]. Some of the hybrid IDS have high computational overhead and high resource consumption. Some of them have a high delay. The remainder of this section is the survey of the chosen papers.

Amin et al. [93] have demonstrated an IDS IP based Ubiquitous Sensor Networks (IPUSN) The proposed method has two segments, Internet Packet Analyzer (IPA) and USN packet analyzer, which is responsible for detecting attacks by analyzing the traffic based on the packet type. The IPA includes two segments including anomaly detector and pattern classifier. Anomaly detector detects the abnormal traffic towards the sensor nodes and pattern classifier is responsible for grouping the attack types such as DoS attack. When queues of intrusion detection methods are overflowed and more packets are not accepted, the IPA starts assessing the incoming traffic and sending it to the anomaly detector. The hybrid scheme runs in this way that the anomaly detector applies tests to check the abnormal behavior. Packet classifier starts its activity if any abnormal behavior is detected and runs the simple pattern matching algorithm to check the predefined attack. If the number of packets sent from a particular protocol exceeds the user-defined threshold, an alarm is raised. The three checking modules and another matching part in the system cause computational overhead. It is assumed that the data passed to the buffer are safe but there is no assurance in the real world. The SENSE simulator is used to evaluate the method. Before the attack, the entropy of the source address is about 2. When the attacker starts to mislead the source addresses, the entropy suddenly changes to 17. When the packet count comes close to 700, it shows that the attacker starts sending more packets. These sudden change notifications are then sent to the analyst. After reviewing the data speed, it is possible to create an attack signal. The false alarm rate, lightweight implementation, and low memory consumption are the merits of the method and the high computational overhead and high delay are the demerits of the method.

Also, Kasinathan et al. [77] have demonstrated a security framework for DoS attacks detection in the IoT. The proposed system uses hybrid IDS for detection of DoS attacks. The method monitors the traffic of the 6LoWPAN network and when an anomaly is recognized in the network, it raises an alarm. When receiving the alarm by DoS protection manager, with the aim of increasing the

Table 8
A side-by-side comparison of the selected specification-based IDS techniques.

References	Main idea	Advantages	Disadvantages
Misra et al. [83]	Detecting of attacks with SOA as a system model in the IoT environment	• Low energy consumption • Low computational overhead • Low power consumption	• Depends on expert admin • High false positive with the wrong specification • High false negative with the wrong specification
Murynets and Jover [49]	Detecting anomalous Short Messaging Service (SMS) activities anomalies with contact-based and volumetric-based methods	• High detection accuracy	• Complex implementation • It is not a real-time intrusion detection
Xia et al. [86]	Detecting internal attacks with A mechanism to incentive the nodes to provide the truthful information	• Good detection accuracy • Low delay	• Depends on expert admin
La et al. [44]	Detecting deceptive attacks in a honeypot-enabled IoT network with the game theoretic model	• Valid for security studies • Flexibility adopted to various networks • High detection accuracy • Real-time intrusion detection	• High additional resources • High converge time
Ahmed and Ko [78]	Diminishing the black hole attacks in RPL networks with an effective mitigation technique	• Increased data delivery rate • Low delay • Low false positive rate • High true positive rate • High detection accuracy	• Can detect only black hole attacks • The high false positive rate increasing the infected nodes • Low true positive rate with increasing the infected nodes • Low detection accuracy by increasing the infected nodes
Le et al. [81]	Detecting topology attacks on RPL by a semi-auto profiling technique	• High detection accuracy • High scalability in large-scale network • High energy efficiency • Low computation overhead • Low storage overhead	• High overhead
Surendar and Umamakeswari [91]	Detecting sinkhole attacks with a specification-based intrusion detection technique	• Low overhead • Low energy consumption • High detection accuracy • low false positive rate	• Depending on expert admin • It is not real-time
Fu et al. [2]	Detecting attacks with a uniform intrusion detection method for the IoT networks based on an automata model	• It is real-time IDS • Easy to implement • Low complexity	• Low detection accuracy • High resource consumption • High false positive rate
Gara et al. [1]	Detecting selective forwarding attacks with an IDS that combines Sequential probability ratio test with an adaptive threshold of acceptable probability of dropped packets	• High detection accuracy • High true positive rate	• High communication overhead • High latency • High resource consumption • High false positive rate
Liu, Xu, Zhang, and Wu	Detecting attacks by the SFC and PCA algorithms	• High adaptability • High detection accuracy • Low detection accuracy • Low false alarm rate	• The efficiency decreased with the increase of data volume

accuracy of attack detection and decreasing false alarm rate, it uses the information presented by other network manager component in order to confirm the attack. DoS protection manager takes the network related information from other modules of the network manager layer to check the intrusion. The hybrid scheme is done when the IDS monitors the network traffic and an anomaly is detected in order to defined metrics. The signatures are preloaded to the database, and then the attack can be detected. The performance evaluation of the proposed method is performed using the penetration testing system. The architecture of the proposed is real-time IDS and also offers a low false alarm rate and high true positive rates. But, it is not compactable to general network architecture and it is restricted when the topology of the network is dynamic. Also, it is not clear how the signatures database will be updated.

Raza et al. [26] have outlined, executed, and assessed a SVELTE for the IoT for detecting the routing attacks. The proposed method includes three modules. The 6LoWPAN Mapper (6Mapper) is introduced as the first module to collect information about RPL and rebuild the network in the 6BR. Analyzing the mapped data and detecting intrusion are done by the second module. The distributed mini-firewall can block the well-known attackers by specified patterns, which manually are added by the network administrator. The available nodes in the network can be distinguished by the RPL routing table in the RPL DODAG root. In the RPL, the rank of the child must be greater than the parent, therefore, if a parent has a greater amount rank from the child node, then a graph inconsistency occurs. The distributed mini-firewall as the third module has the task of separating undesirable activities before entering the network. Each module has two lightweight modules inside each node in the IoT. The first one sends mapping data to 6BR, and the latter works with the central firewall. Each constrained node-likewise has a third module to handle end-to-end packet loss. It is adaptable and can be extended out to distinguish more attacks. The proposed strategy is simulated via Contiki OS and Cooja simulator. In the simulation of the proposed method, the Tmote Sky nodes are used. In general, it is anticipated that the 6BR is not a source limited node and can be a computer or a laptop; however, there is currently no equivalent PC 802.15.4 devices, so that 6 Mapper runs on Linux, and communicate with Cooja using the serial socket. For RPL with 6Mapper, each test is executed 10 times, and the mean and standard deviation are calculated to show the accuracy of the results. On the other hand, the experiments with only RPL (no 6Mapper) have no processing intensive components and hence do not require any native parts. Therefore, the experiments only with the RPL similar results are performed. Also, in all experiments, the same seeds are used. Since it does not consider timing inconsistency or bundle misfortune, a

high false positive rate exists. Moreover, when the sink or parent node identifies attacking nodes after route construction, the child node may send information to an attacking node. Consequently, it is essential that more attacking node can choose a legitimate node as its parent in course development.

In addition, Matsunaga et al. [51] have proposed an attack detection method by identifying the timing inconsistency among rank indications of the RPL. The paper investigates the problems of SVELTE based on two proposals. The first proposal declares that each of the nodes in the IoT has the right to hold the last amount of the rank broadcast to the neighboring nodes. In order to avoid the timing inconsistency which causes the rank mismatch; the rank is reported instead of its current rank. The second proposal declares that each node attaches a timestamp to the sink in order to take time inconsistency into consideration. The proposed strategy is simulated via Contiki OS and Cooja simulator. The simulation is performed in a square area of 400 * 400 m. The number of sensor nodes is 32, and the number of attacking nodes is 1 to 4. The false alarm rate of the method is low because of timestamp which used for reporting rank measurements. However, it has high resource consumption.

Sedjelmaci et al. [74] have suggested a new game theoretic model to detect the attackers by merging the upsides of the anomaly and signature-based IDSs. The proposed method uses the game theory and Nash Equilibrium (NE) to activate the anomaly-based IDS when a new attack's signature is likely to occur. Also, by creating the game model of the intruder and normal user, the NE value is calculated and used to decide when to use the intrusion detection method Intrusion detection security system in the proposed method is in the form of a game between the attacker's intrusion and the IDS which has been installed on the devices of the IoT network. As a result, NE is used to forecast the equilibrium state in which the attacker will create a new signature regardless of the action of IDS. TOSSIM simulator is used to evaluate the proposed method. The total simulation time is 900 s in a square area of 300 * 300. The number of sensor nodes is varied from 50 to 300, and the number of attack nodes is varied from 10% to 40% of the total system nodes. Low energy consumption to realize the high-security level, high detection rate, and low false positive rate are upsides of the method. However, the delay of the network is high.

Shreenivas et al. [85] have extended SVELTE, an IDS for the IoT, with an intrusion detection module that uses the Expected Transmissions (ETX) metric. In RPL, an attacker can exploit the ETX metric and can launch different attacks by getting a better position in the RPL Directed Acyclic Graph (DAG). To overcome these attacks and also to find the malicious nodes, ETX-based and geographical detection algorithms have been developed. The 6Mapper traverses through the entire DAG and records features for all the nodes participating in the DAG. Then intruders who advertise false ETX values to gain more strength or to perform DoS attacks have been detected. The ETX values are calculated for every single node and their neighbors. The parent's ETX value should be lower than that of its children. An intruder is determined if any of the ETX values are abnormal. The proposed method with geographic hints can help to mitigate the rank and ETX attacks. The method attempts to cluster the nodes with limitations of their transmission power to find their immediate neighbors. Firstly, the method calculates the transmission limits for every node in the network and maintains a neighbor table listing the identities of the nodes within their transmission range. If a node from a much lower cluster attempts to fake the identity of a node from a much higher cluster, the IDS can identify the node as an intruder. The proposed strategy is simulated via Contiki OS and Cooja simulator. To evaluate the efficiency and simulation of the proposed method, the Tmote sky nodes are used as things in 6LoWPAN networks. The experiments are run on an emulated 6LoWPAN network with RPL as the routing protocol and ContikiMAC as the MAC protocol. The same seeds are used for all measurements. High detection accuracy, high true positive rate, real-time intrusion detection, low power consumption, and low resource consumption are the merits of the method and high false positive rate and high computational overhead are the demerits of the method.

Midi et al. [94] have introduced Kalis, a self-adapting, knowledge-driven expert IDS able to detect attacks in real time across a wide range of IoT systems. Kalis does not apply changes in the existing IoT software and can monitor a wide variety of protocols, has no performance impact on applications on IoT devices, and enables collaborative security scenarios. With these concepts in place, the knowledge-driven intrusion detection approach follows this conceptual process: using observation, the system can determine feature *F* of the monitored entities and network. Given the knowledge about *F*, the system can determine which one(s) among detection methods to activate. When only the right detection techniques are active, they will process the available information to detect the security incidents. The TelosB wireless sensor mote with a custom TinyOS application is used to evaluate the method. The implementation of Kalis is done using java on the Odroid xu3 development board. In order to interact with the IEEE 802.15.4 traffic, we leverage a TelosB wireless sensor mote with a custom TinyOS application as a bridge. Additionally, the tcpdump tool was added to the Kalis tool, which uses the libpcap library to monitor all WiFi traffic. The implementation of the proposed method uses Java Reflection in different parts of the system. This implementation allows adding new modules without having to recompile the whole system as long as these modules execute the required interfaces. High detection accuracy, low CPU usage, low RAM usage, online detection, low false positive rate, and extendibility are the upsides of the method and high computational overhead is the downside of the method.

Finally, Sedjelmaci et al. [90] have proposed a technique based on the game theory that the anomaly –based detection technique is only used when a new attack with a new signature occurs for detecting the intrusion. Each object on the IoT contains IDS and each IDS contains both of the signature-based and anomaly-based IDS. In the signature-based IDS, the activity of the IoT object is compared with the signatures which are stored in the objects of the IoT network and it is related to each attack pattern. The anomaly-based IDS uses a learning method which contains training and classification procedure. The IDS in the training phase observes some metrics of the suspicious IoT object and models its normal and abnormal behavior. In the classification phase, the new metrics of the IoT object are classified into normal and abnormal behavior. Then the IDS creates a rule for the newly detected attack and the threshold is updated, then it is stored in the database in order to use in the signature-based detection phase. The TOSSIM simulator is used to evaluate the efficiency of the method. The portable and static sensors are randomly distributed in an area with (300×300) m^2 dimensions. The portable sensors follow the predetermined paths, as well as random velocities within the interval. The number of attacking nodes varies from 10% to 40% of the total number of simulation space nodes. There are two categories of attacking nodes: *(i)* Attackers with temporary abnormal behaviors that are changing between normal and unusual behaviors. *(ii)* Attackers with abnormal behavior that never changes their behavior. High detection accuracy, lightweight implementation, low latency, low resource consumption, and low false positive rate are upsides of the method and high computational overhead are downsides of it. Table 9 demonstrates a side-by-side comparison of the selected hybrid IDS techniques.

Table 9
A side-by-side comparison of the selected hybrid IDS techniques.

Reference	Main idea	•Advantages	Disadvantages
Amin et al. [93]	Detecting attacks with designing a generalized architecture for IP-USN IDS and implement an IDS based upon the generalized architecture	• Low false alarm rate • Lightweight • Low memory consumption	• High computational overhead • High delay
Kasinathan et al. [77]	The DoS protection manager is proposed using the detection of abnormal behavior and matching with signatures of attacks	• Real-time IDS • Low false alarm rate • High true positive rates • High availability	• Limited in dynamic network topology • It is not clear how the signatures the database will be updated. • High resource consumption
Raza et al. [26]	Targeting the routing attacks with an IDS with integrated mini-firewall which uses anomaly-based IDS in the intrusion detection and signature-based IDS in the mini-firewall	• Real-time intrusion detection • Extendable • Low overhead • High true positive rate	• High false alarm rate • High resource consumption • Low detection accuracy
Matsunaga et al. [51]	Detecting attackers by considering timing inconstancy with broadcasting the latest rank to neighbor nodes and attaching a timestamp to the sink.	• Real-time intrusion detection • High extending • Low overhead • Low false alarm rate • High detection accuracy • High true positive rate	• High resource consumption • High computation overhead
Sedjelmaci et al. [74]	Detecting attackers with a game theoretic model by activating the anomaly detection only when a new attack pattern is expected to occur otherwise signature-based detection activated	• High detection accuracy • Low false positive rates • Low energy consumption • Lightweight	• High delay • High computational cost • High resource consumption
Shreenivas et al. [85]	Detecting attacks by extending the SVELTE with the ETX metric and geographical hints	• High detection accuracy • High true positive rate • Real-time intrusion detection • Low power consumption • Low resource consumption	• High false positive rates • High computational overhead
Midi et al. [94]	Detecting attacks in real-time with a self-adapting, knowledge-driven expert IDS across a wide range of IoT systems	• High detection accuracy • Low CPU usage • Low RAM usage • Online detection • Low false positive rate • Extendible	• High computation overhead
Sedjelmaci et al. [74]	Detecting wormhole, sinkhole, black hole attacks with a game theoretic model.	• High detection accuracy • Lightweight • Low latency • Low false alarm rate • Low resource consumption	• High computational overhead

6. Discussion

In this section, the obtained results from previous sections are evaluated and discussed. Table 10 shows a comparison of IDS techniques in the IoT environment in terms of detection accuracy, false positive rate, resource consumption, real-time capability, scalability, flexibility, and robustness. The first column presents the categories of the intrusion detection technique. The second column shows the papers. The last seven columns are intrusion detection metrics.

Fig. 9 illustrates a pie chart diagram that shows the percentage of IDS metrics in the articles under review. For example, in the 31 papers from 40 reviewed papers, detection accuracy is high. Table 11 shows the percentage of the IDS metrics in each category of the articles under review. The first row shows the detection metrics and the first column presents the categories. The second row shows that the total value is independent of each category that the detection accuracy has the maximum value and the scalability has the least value. In the third row, the maximum value belongs to flexibility and the least belongs to the false positive, robustness and scalability, this is common because the anomaly-based techniques have a high false positive rate. Since the signature-based detection can detect specified attacks, in the signature-based techniques, all of the papers have high detection accuracy. But, in the real IoT environment with several other attacks, the detection accuracy is sharply decreased. In the hybrid IDS, 87.5% of the papers are real-time, 50% belongs to resource consumption; so, we can say that the resource consumption of the hybrid scheme is high because of the complexity of computation. In the specification-based IDS, 70% of the studies have high detection accuracy, but most of them have a high false positive rate and resource consumption.

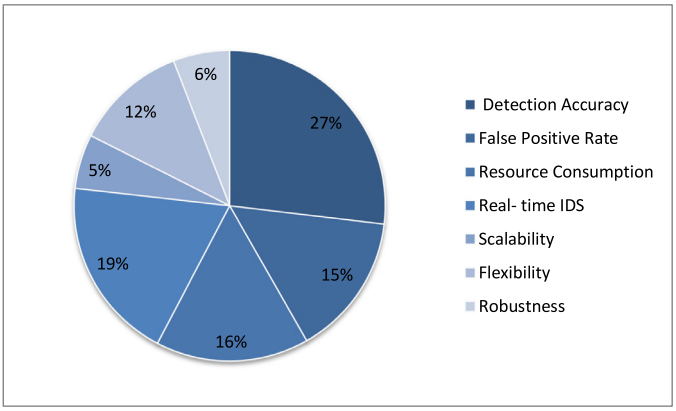

Fig. 9. Percentage of IDS metrics in the reviewed articles.

Fig. 10 shows the categorization of the reviewed studies into three categories based on the location of IDS. The first category is the centralized IDSs. The second category is distributed IDSs and the related studies are also illustrated. It is clear that architecture has been studied in most of the studies. Finally, the third category is hybrid IDS.

Table 10
A comparison of IDS techniques in the IoT environment in terms of detection accuracy, false positive rate, resource consumption real-time capability, scalability, flexibility, and robustness.

Categories	References	Detection accuracy	False positive rate	Resource consumption	Real-time capability	Scalability	Flexibility	Robustness
Anomaly-based IDS	Wang et al. [72]	√	×	×	√	√	√	√
	Ding et al. [75]	√	×	√	×	×	×	×
	Rajasegarar et al. [79]	√	×	×	×	×	√	√
	Chen et al. [82]	×	×	×	√	×	×	√
	Ham et al. [84]	√	√	×	×	×	×	×
	Pongle and Chavan [87]	×	×	√	√	×	×	×
	Cervantes et al. [89]	√	√	×	×	√	×	×
	Summerville et al. [92]	√	√	×	√	√	√	×
	Fu et al. [16]	×	√	√	×	×	√	×
	Eliseev and Gurina [96]	×	×	√	×	×	×	×
	Rahman et al. [95]	√	×	×	×	×	×	×
	Zhang and Green [97]	×	×	×	×	×	×	×
	Grgic et al. [98]	√	×	√	√	×	√	×
	Sonar and Upadhyay [99]	√	√	×	×	×	×	×
	Hodo et al. [100]	√	√	×	√	×	×	×
	Khan and Herrmann [101]	√	×	√	√	×	√	×
	Lopez-Martin et al. [102]	√	×	√	√	×	√	×
	Diro and Chilamkurti [88]	√	√	√	×	×	×	×
	Shi et al. [103]	√	×	×	√	×	×	×
	Li et al. [104]	√	√	√	×	×	√	√
	Pamukov et al. [105]	√	√	×	×	√	×	×
Signature- based IDS	Sun et al. [73]	√	×	×	√	×	×	×
	Oh et al. [76]	√	×	√	×	√	×	×
	Amin et al. [80]	√	√	√	×	×	×	×
Specification-based IDS	La et al. [44]	√	×	×	√	×	√	×
	Ahmed and Ko [78]	√	√	×	√	×	×	×
	Misra et al. [83]	×	×	√	×	×	×	×
	Le et al. [81]	√	×	√	×	√	×	√
	Xia et al. [86]	√	×	×	√	×	×	×
	Murynets and Jover [49]	√	×	×	×	×	×	√
	Surendar and Umamakeswari [91]	√	√	√	√	×	×	×
	Fu et al. [2]	×	×	×	√	×	×	√
	Gara et al. [1]	√	×	×	×	×	×	×
	Liu, Xu, Zhang, and Wu	×	×	√	√	√	×	×
Hybrid	Sedjelmaci et al. [74]	√	√	×	√	×	×	×
	Kasinathan et al. [77]	√	√	×	√	×	√	×
	Raza et al. [26]	×	×	×	√	×	√	×
	Shreenivas et al. [85]	√	×	√	√	×	×	×
	Matsunaga et al. [51]	√	√	×	√	×	√	×
	Amin et al. [93]	×	√	√	×	×	×	×
	Midi et al. [94]	√	√	√	√	×	√	×
	Sedjelmaci et al. [90]	√	√	√	√	×	×	×

Table 11
Percentage of the IDS metrics in each category of the articles under review.

Category	Detection accuracy	False positive rate	Resource consumption	Real-time	Scalability	Flexibility	Robustness
Total	76%	42%	45%	54%	16%	33%	16.6%
Anomaly-based IDS	76%	42%	42%	42%	19%	38%	19%
Signature-based IDS	100%	33%	66%	33%	33%	33%	0%
Hybrid IDS	75%	75%	50%	87.5%	0%	50%	0%
Specification-based IDS	70%	20%	40%	60%	20%	10%	30%

Table 12 shows the categorization of the discussed papers based on the evaluation techniques. The first category is a simulation and sub-categories are various types of simulation software. Another category is a theoretical evaluation which uses formal or other calculations by using the datasets to the assessment of the proposed method.

Table 13 demonstrates the categorization of the discussed papers based on attacks types in 9 categories. Categories in this figure from left to right are DoS, Sybil, Replay, Selective Forwarding, Wormhole, Black Hole, Sinkhole, Jamming, and False Data attacks.

7. Open issues and future trends

This section offers major IDSs issues that have not been broadly and thoroughly studied as yet, as research directions in the future. Emphasizing the fundamental performance metrics of intrusion detection and application evolvement of these metrics over time is indispensable to make practical decisions regarding intrusion detection. Apparently, the implementation of intrusion detection in the IoT is hard because the things in the IoT are resource-constrained devices. The low-cost and low-quality sensor nodes have inflexible constraints such as energy, memory, computational capacity, and communication. Most of the conventional IDSs have given limited attention to the availability of computational resources. They are computationally costly and need much memory for data examination and storage. In this manner, designing IDS is needed to decrease resource consumption by using a sensible measure of memory for storage and computational operations. Then when the IDSs are applied without focusing on the consumption instruction of resources in the constrained

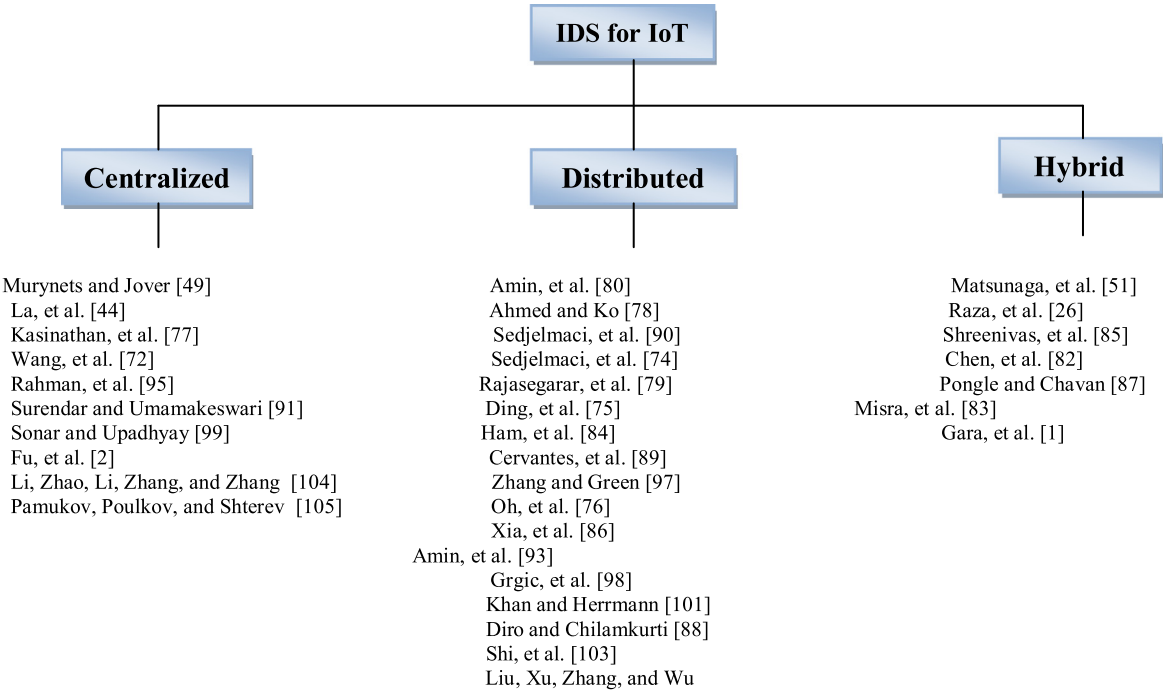

Fig. 10. IDS for IoT; categorization based on the location of IDS.

Table 12
IDS for IoT; categorization based on evaluation techniques.

IDS for IoT	Simulation	C/C++	Sun et al. [73], Hodo et al. [100]
		Contiki/Cooja	Pongle and Chavan [87], Zhang and Green [97], Cervantes et al. [89], Grgic et al. [98], Ahmed and Ko [78], Le et al. [81], Raza et al. [26], Shreenivas et al. [85], Matsunaga et al. [51], Sonar and Upadhyay [99], Shi et al. [103], Gara et al. [1]
		MATLAB	Wang et al. [72], Rahman et al. [95], Eliseev and Gurina [96], La et al. [44], Xia et al. [86], Khan and Herrmann [101], Pamukov et al. [105]
		SENSE / Raspberry Pi / NS/TelosB / TineyOS / TOSSIM	Sedjelmaci et al. [74], Sedjelmaci et al. [90], Amin et al. [93], Oh et al. [76], Kasinathan et al. [77], Surendar and Umamakeswari [91], Fu et al. [2]
	Theoretical	Ding et al. [75], Rajasegarar et al. [79], Chen et al. [82], Summerville et al. [92], Murynets and Jover [49] Fu et al. [16], Amin et al. [80], Lopez-Martin et al. [102], Diro and Chilamkurti [88], Hodo et al. [100]	

devices, the likelihood of stopping the system is fundamentally expanding.

Furthermore, most of the vitality in the IoT is focused on communication. For a sensor node, the communication cost is sometimes more than the computation cost [72,110]. A large portion of conventional outlier IDSs utilizing a centralized approach for data analysis causes an excessive amount of communication overhead. In this manner, a test for anomaly detection in the IoT can minimize the communication overhead, reduce the network traffic and extend the lifetime of the network.

Further, deployed sensor networks can have a gigantic size (up to hundreds or even a huge number of sensor nodes). The key challenge of customary IDSs is to keep up a high detection rate while keeping the false alarm rate low. This requires the development of a precise normal profile that presents the normal behavior of sensor data [72,110]. This is an exceptionally troublesome undertaking for large-scale sensor organized applications. Moreover, traditional IDSs do not scale well to process an expansive measure of distributed data streams in an online way [111].

Additionally, an extensive number of techniques that have been proposed in the IoT can identify little numbers of attacks. This is an issue that some creators can work on IDSs equipped for distinguishing the majority of the attacks. In anomaly-based IDSs, the preparation and testing time to accomplish normal behavior of the network is high. Then the detection of the intrusion continuously is unimaginable and if the training dataset is being smaller, the IDS cannot accomplish the normal behavior of the IoT network. Therefore, designing an IDS which able to cope with these problems is a challenge.

Also, as indicated by the particular attributes of IoT, lightweight IDSs would dependably be the future research heading. So, the scientists need to study lightweight solutions for IoT framework to meet the particular prerequisites of the particular application. Then designing an IDS which suggests lightweight computation complexity is a prerequisite and distinctive security necessities.

Although the RPL standard contains some versions using simple security methods to route control messages in the IoT security, it suffers from having a fundamental system for supporting essential safe routing processes. Falsification attacks, routing information, reply, Byzantine attacks, physical device compromise, remote device access attacks, selective forwarding attacks, black and gray hole attacks, and version number manipulation attacks, are threatening the RPL [112–114]. Except for the safe adaptations of the routing control messages, no further security methods are composed in the present version of the RPL protocol standard [114]. In this regard, many researches might be centered around the meaning of threat models for RPL, which is suitable for specific application areas.

There are almost no detailed simulations for the discussed IDS mechanisms. Most of the papers do not offer complete discussion or simulations. Furthermore, the effectiveness of most IDSs is difficult to investigate because of the lack of real network traces. There

Table 13
IDS for IoT; categorization based on attacks.

	DoS/DDoS	Sybil	Replay	Selective Forwarding	Wormhole	Black Hole	Sinkhole	Jamming	False Data
Wang et al. [72]	√					√			
Ding et al. [75]				√					
Pongle and Chavan [87]					√				
Cervantes et al. [89]							√		
Summerville et al. [92]	√								
Fu et al. [16]	√								
Rahman et al. [95]	√								
Zhang and Green [97]	√								
Grgic et al. [98]	√	√			√		√		
Sonar and Upadhyay [99]	√								
Hodo et al. [100]	√								
Khan and Herrmann [101]	√			√			√		
Diro and Chilamkurti [88]	√								
Shi et al. [103]		√					√		
Sun et al. [73]	√								
Amin et al. [80]	√								
La et al. [44]									
Ahmed and Ko [78]						√	√		
Misra et al. [83]	√								
Le et al. [81]	√								
Murynets and Jover [49]	√								
Surendar and Umamakeswari [91]								√	
Fu et al. [2]								√	√
Gara et al. [1]				√					
Sedjelmaci et al. [74]	√								
Kasinathan et al. [77]	√								
Raza et al. [26]				√			√		
Shreenivas et al. [85]							√		
Matsunaga et al. [51]				√			√		
Amin et al. [93]	√								
Midi et al. [94]				√					
Sedjelmaci et al. [90]		√			√	√	√		
Rajasegarar et al. [79]									√
Li et al. [104]	√								
Pamukovet al. [105]	√								

are little numbers of real-world implementations of IDS mechanisms in the IoT. Statistical assesses and simulations are vital to verify the efficiency of the IDS mechanisms in a real setting attack resistant packaging. The things in the IoT environment might be distributed in remote areas and unprotected. The possibility of conquering devices in the IoT is done by the attackers. Then they can exploit the cryptographic secrets, adjust programs, or replace them with malicious nodes. Tamper resistant packaging in designing IDS can defend against these intrusions.

The IoT devices can join or leave a network anytime from anyplace. A network topology becomes dynamic by the temporal and spatial device adding and leaving feature. The available IDSs do not adapt to these kinds of sudden network topological changes. Therefore, since these methods do not have the ability to secure the IoT device completely, it is a very good line for future researches. Furthermore, using least-squares support-vector machine (LSSVM) [115] for improving the reviewed SVM-based method can be investigated.

Furthermore, investigating the formal verification and behavioral modeling [116,117] of the reviewed techniques are very interesting lines for future research. Finally, investigation the combination of some meta-heuristic algorithms such as Particle Swarm Optimization (PSO) [118–120], bee colony [121,122], differential evolution [123], mixed integer genetic algorithm [124], harmony search [125], world cup optimization algorithm [126], imperialist competitive algorithm [127,128] with neural networks [129,130] and fuzzy logic [131–134] for designing the powerful IDSs is very interesting line for future research.

8. Limitation

In the current paper, an SLR on IDSs in the IoT environment has been presented, but it might have some deficiencies. Therefore, the limitations of the current study must be considered in future studies as follows:

- Research scope: The IoT has been investigated in several sources such as academic publications, technical reports, editorial notes, and web pages and the academic major international journals and conferences should be included to obtain the best qualification. Specifically, papers published in national journals and conferences are eliminated.
- Study and publication bias: We selected 14 databases as reliable electronic databases. In fact, these sites contain the best articles on the IoT. But, there is a likelihood that some suitable articles are ignored through this restraint.
- Classification: We categorized papers in four categories, but it can be categorized in other ways, too. Furthermore, we found a paper which is proposed by [135] that proposed a hybrid method of specification-based and anomaly-based IDSs. But, because that paper is the only paper that we can find in the hybrid method of anomaly and specification-based, then we have to ignore it.

9. Summary and conclusion

This study has proposed a systematic review of IDSs in IoT environments. In a resembling way, we have reviewed numerous highly developed intrusion detection in the IoT, clarifying and discussing open issues via an in-depth analysis of over 40 main studies among the basic 324 papers. Based on the accessible literature, the found papers are categorized into four main categories including anomaly-based IDS, signature-based IDS, specification-based IDS, hybrid IDS and also three categories including centralized, distributed, and hybrid. Further, two categories of evaluation (simulation, theoretical) and nine categories of attacks (DoS/DDoS,

selective forwarding, Sybil, sinkhole, wormhole, jamming, false data, replay, black hole) are considered. We also discussed the upsides and downsides related to many IDSs. The challenges of these techniques are addressed so that more efficient IDSs can be developed in the future. Proper IDS has the ability to keep minimum resource consumption, minimum false alarm rate, maximum detection accuracy, real-time intrusion detection, high scalability, high flexibility, and high robustness. In general, IDSs in the IoT environment still needs improvements in terms of increasing detection accuracy, true positive rate, and energy consumption.

The obtained results also have shown the detection accuracy has the maximum amount of 27% and the scalability has the least amount of 5%. After an assessment of the results of the localization of the IDSs, we see that 31% of the studies are centralized, 50% are distributed, and 18.75% is a hybrid. After collecting information about the evaluation technique of studies, 72% of the papers use simulation techniques and 27% use theoretical techniques. In the simulation-based papers, 44% of the papers use Contiki/Cooja, 7% C/C++, 50% use other simulation tools. According to the distinguishable attacks, 60% of the papers detect the DoS attacks. We can say that most of the papers are about the detection of DoS attacks. Minimum numbers of the papers are about the detection of other types of attacks. The overall data collected in this study help to introduce the researchers with high developed studies in the IDS area. Totally, the answers to the definitional questions summarize the intrusion detection's primary purpose, current challenges, open issues, and approaches in the IoT

Conflict of interest

The authors have declared no conflict of interest.

References

[1] F. Gara, L.B. Saad, R.B. Ayed, An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs, in: *Proceedings of the 2017 13th International* Wireless Communications and Mobile Computing Conference *(IWCMC)*, IEEE, 2017, pp. 276–281.

[2] Y. Fu, Z. Yan, J. Cao, O. Koné, X. Cao, An automata based intrusion detection method for internet of things, Mob. Inf. Syst. 2017 (2017) 1–13.

[3] Z. Ghanbari, N.J. Navimipour, M. Hosseinzadeh, A. Darwesh, Resource allocation mechanisms and approaches on the Internet of Things, Cluster Comput. (2019) 1–30.

[4] M. Hamzei, N.J. Navimipour, Toward efficient service composition techniques in the Internet of Things, IEEE Int. Things J. 5 (5) (2018) 3774–3787.

[5] S. Sarma, "Brock. D. The Internet of Things, White Paper, Auto-ID center," ed: MIT, 1998.

[6] L. Coetzee, J. Eksteen, The Internet of Things-promise for the future? An introduction, in: IST-Africa Conference Proceedings, 2011, IEEE, 2011, pp. 1–9.

[7] A.R. Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the internet of things, Digital Commun. Netw. 4 (2) (2018) 118–137.

[8] D. Uckelmann, M. Harrison, F. Michahelles, An Architectural Approach Towards the Future Internet of Things, Springer, 2011.

[9] B. Pourghebleh, N.J. Navimipour, Data aggregation mechanisms in the internet of things: a systematic review of the literature and recommendations for future research, J. Netw. Comput. Appl. 97 (2017) 23–34.

[10] N. Council, Six technologies with potential impacts on US interests out to 2025, in: *Proceedings of the* Disruptive Civil Technologies, 2008, 2008.

[11] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[12] J. Du, S. Chao, A study of information security for M2M of IOT, in: Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 3, IEEE, 2010 V3-576-V3-579.

[13] J.-H. Lee, H. Kim, Security and privacy challenges in the internet of things [security and privacy matters], IEEE Consum. Electr. Mag. 6 (3) (2017) 134–136.

[14] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wirel. Netw. 20 (8) (2014) 2481–2501.

[15] H. Ning, H. Liu, L.T. Yang, Cyberentity security in the internet of things, Computer 4 (2013) 46–53.

[16] R. Fu, K. Zheng, D. Zhang, Y. Yang, An intrusion detection scheme based on anomaly mining in Internet of Things, in: Proceedings of the 4th IET International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2011), IET, 2011, pp. 315–320.

[17] B. Mbarek, A. Meddeb, W.B. Jaballah, M. Mosbah, A secure authentication mechanism for resource constrained devices, in: Proceedings of the 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), IEEE, 2015, pp. 1–7.

[18] C. Jun, C. Chi, Design of complex event-processing IDS in internet of things, in: Proceedings of the 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, IEEE, 2014, pp. 226–229.

[19] H. Ning, H. Liu, Cyber-physical-social based security architecture for future internet of things, Adv. Int. Things 2 (01) (2012) 1.

[20] W.H. Inmon, D. Strauss, G. Neushloss, DW 2.0: The Architecture for the Next Generation of Data Warehousing, Morgan Kaufmann, 2010.

[21] C.M. Liu, Y. Zhang, R. Chen, L.X. Xiao, J.D. Zhang, Research on intrusion detection for the internet of things based on clone selection principle, in: Proceedings of the Advanced Materials Research, 562, Trans Tech Publ., 2012, pp. 1982–1985.

[22] I. Onat, A. Miri, An intrusion detection system for wireless sensor networks, in: Proceedings of the IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005 (WiMob'2005), 3, IEEE, 2005, pp. 253–259.

[23] K. Ioannis, T. Dimitriou, F.C. Freiling, Towards intrusion detection in wireless sensor networks, in: Proceedings of the 13th European Wireless Conference, Citeseer, 2007, pp. 1–10.

[24] S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, Quarter sphere based distributed anomaly detection in wireless sensor networks, in: Proceedings of the 2007 IEEE International Conference on Communications, IEEE, 2007, pp. 3864–3869.

[25] S. Rajasegarar, C. Leckie, M. Palaniswami, Anomaly detection in wireless sensor networks, IEEE Wirel. Commun. 15 (4) (2008) 34–40.

[26] S. Raza, L. Wallgren, T. Voigt, SVELTE: real-time intrusion detection in the internet of things, Ad Hoc Netw. 11 (8) (2013) 2661–2674.

[27] A. Rghioui, A. Khannous, M. Bouhorma, Denial-of-service attacks on 6LoWPAN-RPL networks: threats and an intrusion detection system proposition, J. Adv. Comput. Sci. Technol. 3 (2) (2014) 143.

[28] B. Pourghebleh, N. Jafari Navimipour, Towards efficient data collection mechanisms in the vehicular ad hoc networks, Int. J. Commun. Syst. 32 (5) (2019) e3893.

[29] B. Hajimirzaei, N.J. Navimipour, Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm, ICT Express 5 (1) (2019) 56–59.

[30] Y. Ebadi, N. Jafari Navimipour, An energy-aware method for data replication in the cloud environments using a Tabu search and particle swarm optimization algorithm, Concurr. Comput. Pract. Exp. 31 (1) (2019) e4757.

[31] S. Owais, V. Snasel, P. Kromer, A. Abraham, Survey: using genetic algorithm approach in intrusion detection systems techniques, in: Proceedings of the 2008 7th Computer Information Systems and Industrial Management Applications, IEEE, 2008, pp. 300–307.

[32] W. Li, Using genetic algorithm for network intrusion detection, in: Proceedings of the United States Department of Energy Cyber Security Group, 1, 2004, pp. 1–8.

[33] P. Wang, L. Shi, B. Wang, Y. Wu, Y. Liu, Survey on HMM based anomaly intrusion detection using system calls, in: Proceedings of the 2010 5th International Conference on Computer Science & Education, IEEE, 2010, pp. 102–105.

[34] R.G.M. Helali, Data mining based network intrusion detection system: a survey, in: Proceedings of the Novel Algorithms and Techniques in Telecommunications and Networking, Springer, 2010, pp. 501–505.

[35] C. Kolias, G. Kambourakis, M. Maragoudakis, Swarm intelligence in intrusion detection: a survey, Comput. Secur. 30 (8) (2011) 625–642.

[36] T. Sherasiya, H. Upadhyay, H. b. Patel, A survey: intrusion detection system for internet of things, Int. J. Comput. Sci. Eng. 1 (5) (2016) 81–90.

[37] A.A. Gendreau, M. Moorman, Survey of intrusion detection systems towards an end to end secure internet of things, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2016, pp. 84–90.

[38] B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in Internet of Things, J. Netw. Comput. Appl. 84 (2017) 25–37.

[39] T. Borgohain, U. Kumar, S. Sanyal, Survey of security and privacy issues of internet of things, 2015 arXiv preprint arXiv:1501.02211.

[40] M. Ammar, G. Russello, B. Crispo, Internet of things: a survey on the security of IoT frameworks, J. Inf. Secur. Appl. 38 (2018) 8–27.

[41] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, IEEE Int. Things J. 4 (5) (2017) 1250–1258.

[42] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: a top–down survey, Comput. Netw. 141 (2018) 199–221.

[43] M. Usha, P. Kavitha, Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier, Wirel. Netw. 23 (8) (2017) 2431–2446.

[44] Q.D. La, T. Quek, J. Lee, S. Jin, H. Zhu, Deceptive attack and defense game in honeypot-enabled networks for the internet of things, IEEE Int. Things J. 3 (6) (2016) 1025–1035.

[45] M. De Jonge, J. Muskens, M. Chaudron, Scenario-based prediction of run-time resource consumption in component-based software systems, in: Proceedings of the 6th ICSE Workshop on Component Based Software Engineering: Automated Reasoning and Prediction, Citeseer, 2003.

[46] T.F. Lunt, A. Tamaru, F. Gillham, A Real-Time Intrusion-Detection Expert System (IDES), SRI International. Computer Science Laboratory, 1992.

[47] S. Kumar, K. Dutta, Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges, Secur. Commun. Netw. 9 (14) (2016) 2484–2556.

[48] E.H. Spafford, D. Zamboni, Intrusion detection using autonomous agents, Comput. Netw. 34 (4) (2000) 547–570.

[49] I. Murynets, R.P. Jover, Anomaly detection in cellular machine-to-machine communications, in: Proceedings of the 2013 IEEE International Conference on Communications (ICC), IEEE, 2013, pp. 2138–2143.
[50] N. Einwechter, "An introduction to distributed intrusion detection systems," Security Focus, 2001.
[51] T. Matsunaga, K. Toyoda, I. Sasase, Low false alarm attackers detection in RPL by considering timing inconstancy between the rank measurements, IEICE Commun. Express 4 (2) (2015) 44–49.
[52] J. Lin. An analysis on DoS attack and defense technology. In: 7th International Conference on Computer Science & Education (ICCSE). IEEE, 2012. DOI: 10.1109/ICCSE.2012.6295258.
[53] J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: analysis & defenses, in: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, ACM, 2004, pp. 259–268.
[54] M.A. Jan, P. Nanda, X. He, R.P. Liu, A Sybil attack detection scheme for a centralized clustering-based hierarchical network, in: Proceedings of the Trustcom/BigDataSE/ISPA, 2015, 1, IEEEIEEE, 2015, pp. 318–325.
[55] A. Teixeira, D. Pérez, H. Sandberg, K.H. Johansson, Attack models and scenarios for networked control systems, in: Proceedings of the 1st international conference on High Confidence Networked Systems, ACM, 2012, pp. 55–64.
[56] B. Yu, B. Xiao, Detecting selective forwarding attacks in wireless sensor networks, in: Proceedings of the 20th International Parallel and Distributed Processing Symposium, 2006. IPDPS 2006, IEEE, 2006, p. 8.
[57] P. Goyal, S. Batra, A. Singh, A literature review of security attack in mobile ad-hoc networks, Int. J. Comput. Appl. 9 (12) (2010) 11–15.
[58] A. Mathur, T. Newe, M. Rao, Defence against black hole and selective forwarding attacks for medical WSNs in the IoT, Sensors 16 (1) (2016) 118.
[59] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Trans. Inf. Syst. Secur. (TISSEC) 14 (1) (2011) 13.
[60] F. Aznoli, N.J. Navimipour, Deployment strategies in the wireless sensor networks: systematic literature review, classification, and current trends, Wirel. Person. Commun. 95 (2) (2017) 819–846.
[61] F. Aznoli, N.J. Navimipour, Cloud services recommendation: reviewing the recent advances and suggesting the future research directions, J. Netw. Comput. Appl. 77 (2017) 73–86.
[62] P.F. Buller, G.M. McEvoy, Strategy, human resource management and performance: sharpening line of sight, Hum. Resour. Manag. Rev. 22 (1) (2012) 43–56.
[63] M. Chiregi, N.J. Navimipour, A comprehensive study of the trust evaluation mechanisms in the cloud computing, J. Serv. Sci. Res. 9 (1) (2017) 1–30.
[64] E. Fraj, J. Matute, I. Melero, Environmental strategies and organizational competitiveness in the hotel industry: the role of learning and innovation as determinants of environmental success, Tour. Manag. 46 (2015) 30–42.
[65] A. Vakili, N.J. Navimipour, Comprehensive and systematic review of the service composition mechanisms in the cloud environments, J. Netw. Comput. Appl. 81 (2017) 24–36.
[66] S. Keele, Guidelines for performing systematic literature reviews in software engineering, Technical report, Ver. 2.3 EBSE Technical Report. EBSE, 5, 2007.
[67] B.A. Milani, N.J. Navimipour, A systematic literature review of the data replication techniques in the cloud environments, Big Data Res. 10 (2017) 1–7.
[68] A.S. Milani, N.J. Navimipour, Load balancing mechanisms and techniques in the cloud environments: systematic literature review and future trends, J. Netw. Comput. Appl. 71 (2016) 86–98.
[69] A.A. Neghabi, N.J. Navimipour, M. Hosseinzadeh, A. Rezaee, Load balancing mechanisms in the software defined networks: a systematic and comprehensive review of the literature, IEEE Access 6 (2018) 14159–14178.
[70] A. Isfandyari-Moghaddam, M.-K. Saberi, The life and death of URLs: the case of journal of the medical library association, Libr. Philos. Pract. 7 (2011) 1–8.
[71] M.K. Saberi, Open Access Journals with a view of journals covered in ISI, Inf. Sci. Tech. 24 (2) (2009) 105–122.
[72] J. Wang, Q. Kuang, S. Duan, A new online anomaly learning and detection for large-scale service of Internet of Thing, Person. Ubiquitous Comput. 19 (7) (2015) 1021–1031.
[73] H. Sun, X. Wang, R. Buyya, J. Su, CloudEyes: cloud-based malware detection with reversible sketch for resource-constrained internet of things (IoT) devices, Softw. Pract. Exp. (2016).
[74] H. Sedjelmaci, S.M. Senouci, M. Al-Bahri, A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology, in: Proceedings of the 2016 IEEE International Conference on Communications (ICC), IEEE, 2016, pp. 1–6.
[75] Y. Ding, X.-W. Zhou, Z.-M. Cheng, F.-H. Lin, A security differential game model for sensor networks in context of the internet of things, Wirel. Pers. Commun. 72 (1) (2013) 375–388.
[76] D. Oh, D. Kim, W.W. Ro, A malicious pattern detection engine for embedded security systems in the Internet of Things, Sensors 14 (12) (2014) 24188–24211.
[77] P. Kasinathan, C. Pastrone, M.A. Spirito, M. Vinkovits, Denial-of-service detection in 6LoWPAN based internet of things, in: Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2013, pp. 600–607.
[78] F. Ahmed, Y.B. Ko, Mitigation of black hole attacks in routing protocol for low power and lossy networks, Secur. Commun. Netw. (2016).
[79] S. Rajasegarar, et al., Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained networks, Pattern Recognit. 47 (9) (2014) 2867–2879.
[80] S.O. Amin, M.S. Siddiqui, C.S. Hong, J. Choe, A novel coding scheme to implement signature based IDS in IP based sensor networks, in: Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management–Workshops, 2009. IM'09., IEEE, 2009, pp. 269–274.
[81] A. Le, J. Loo, K.K. Chai, M. Aiash, A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology, Information 7 (2) (2016) 25.
[82] P.-Y. Chen, S.-M. Cheng, K.-C. Chen, Information fusion to defend intentional attack in internet of things, IEEE Int. Things J. 1 (4) (2014) 337–348.
[83] S. Misra, P.V. Krishna, H. Agarwal, A. Saxena, M.S. Obaidat, A learning automata based solution for preventing distributed denial of service in Internet of things, in: Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (iThings/CPSCom), IEEE, 2011, pp. 114–122.
[84] H.-S. Ham, H.-H. Kim, M.-S. Kim, M.-J. Choi, Linear SVM-based android malware detection for reliable IoT services, J. Appl. Math. 2014 (2014) 1–10.
[85] D. Shreenivas, S. Raza, T. Voigt, Intrusion detection in the RPL-connected 6LoWPAN networks, in: Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, ACM, 2017, pp. 31–38.
[86] Y. Xia, H. Lin, L. Xu, An AGV mechanism based secure routing protocol for internet of things, in: Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), IEEE, 2015, pp. 662–666.
[87] P. Pongle, G. Chavan, Real time intrusion and wormhole attack detection in internet of things, Int. J. Comput. Appl. 121 (9) (2015) 1–9.
[88] A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Gener. Comput. Syst. 82 (2018) 761–768.
[89] C. Cervantes, D. Poplade, M. Nogueira, A. Santos, Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things, in: Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE, 2015, pp. 606–611.
[90] H. Sedjelmaci, S.-m. Senouci, T. Taleb, An accurate security game for low-resource IoT devices, IEEE Trans. Veh. Technol. 66 (10) (2017) 9381–9393.
[91] M. Surendar, A. Umamakeswari, InDReS: an intrusion detection and response system for internet of things with 6LoWPAN, in: Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, 2016, pp. 1903–1908.
[92] D.H. Summerville, K.M. Zach, Y. Chen, Ultra-lightweight deep packet anomaly detection for Internet of Things devices, in: Proceedings of the 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), IEEE, 2015, pp. 1–8.
[93] S.O. Amin, Y. jig Yoon, M.S. Siddiqui, C.S. Hong, A novel intrusion detection framework for IP-based sensor networks, in: Proceedings of the International Conference on Information Networking, 2009. ICOIN 2009, IEEE, 2009, pp. 1–3.
[94] D. Midi, A. Rullo, A. Mudgerikar, E. Bertino, Kalis—a system for knowledge–driven adaptable intrusion detection for the internet of things, in: Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)„ IEEE, 2017, pp. 656–666.
[95] S. Rahman, S. Al Mamun, M.U. Ahmed, M.S. Kaiser, PHY/MAC layer attack detection system using neuro-fuzzy algorithm for IoT network, in: Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), IEEE, 2016, pp. 2531–2536.
[96] V. Eliseev, A. Gurina, Algorithms for network server anomaly behavior detection without traffic content inspection, in: Proceedings of the 9th International Conference on Security of Information and Networks, ACM, 2016, pp. 67–71.
[97] C. Zhang, R. Green, Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network, in: Proceedings of the 18th Symposium on Communications & Networking, Society for Computer Simulation International, 2015, pp. 8–15.
[98] K. Grgic, D. Zagar, V. Krizanovic Cik, System for malicious node detection in IPv6-based wireless sensor networks, J. Sens. 2016 (2016).
[99] K. Sonar, H. Upadhyay, An approach to secure internet of things against DDoS, in: Proceedings of International Conference on ICT for Sustainable Development, Springer, 2016, pp. 367–376.
[100] E. Hodo, et al., Threat analysis of IoT networks using artificial neural network intrusion detection system, in: Proceedings of the 2016 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2016, pp. 1–6.
[101] Z.A. Khan, P. Herrmann, A trust based distributed intrusion detection mechanism for internet of things, in: Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)„ IEEE, 2017, pp. 1169–1176.
[102] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, J. Lloret, Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT, Sensors 17 (9) (2017) 1967.
[103] Y. Shi, T. Li, R. Li, X. Peng, P. Tang, An immunity-based iot environment security situation awareness model, J. Comput. Commun. 5 (07) (2017) 182.
[104] J. Li, Z. Zhao, R. Li, H. Zhang, T. Zhang, AI-based two-stage intrusion detection for software defined IoT networks, IEEE Int. Things J. (2018).
[105] M.E. Pamukov, V.K. Poulkov, V.A. Shterev, Negative selection and neural network based algorithm for intrusion detection in IoT, in: Proceedings of the 2018 41st International Conference on Telecommunications and Signal Processing (TSP), IEEE, 2018, pp. 1–5.

[106] Z. Chen, C. Ji, An information-theoretic view of network-aware malware attacks, IEEE Trans. Inf. Forensics Secur. 4 (3) (2009) 530–541.
[107] R. Sekar, et al., Specification-based anomaly detection: a new approach for detecting network intrusions, in: Proceedings of the 9th ACM conference on Computer and communications security, ACM, 2002, pp. 265–274.
[108] F. Shabestari, A.M. Rahmani, N.J. Navimipour, S. Jabbehdari, A taxonomy of software-based and hardware-based approaches for energy efficiency management in the Hadoop, J. Netw. Comput. Appl. 126 (2019) 162–177.
[109] L. Liu, B. Xu, X. Zhang, X. Wu, An intrusion detection method for internet of things based on suppressed fuzzy clustering, EURASIP J. Wirel. Commun. Netw. (1) (2018) 113 2018.
[110] Y. Zhang, N. Meratnia, P.J. Havinga, Outlier detection techniques for wireless sensor networks: a survey, IEEE Commun. Surv. Tutor. 12 (2) (2010) 159–170.
[111] Q.D. La, T.Q. Quek, J. Lee, A game theoretic model for enabling honeypots in IoT networks, in: Proceedings of the 2016 IEEE International Conference on Communications (ICC), IEEE, 2016, pp. 1–6.
[112] L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the RPL-based internet of things, Int. J. Distrib. Sens. Netw. 9 (8) (2013) 794326.
[113] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A security threat analysis for the routing protocol for low-power and lossy networks (rpls)," 2070-1721, 2015.
[114] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, J. Schönwälder, A study of RPL DODAG version attacks, in: Proceedings of the IFIP international conference on autonomous infrastructure, management and security, Springer, 2014, pp. 92–104.
[115] R. Razavi, M.N. Kardani, A. Ghanbari, M.J. Lariche, A. Baghban, Utilization of LSSVM algorithm for estimating synthetic natural gas density, Pet. Sci. Technol. 36 (11) (2018) 807–812.
[116] B. Keshanchi, A. Souri, N.J. Navimipour, An improved genetic algorithm for task scheduling in the cloud environments using the priority queues: formal verification, simulation, and statistical testing, J. Syst. Softw. 124 (2017) 1–21.
[117] A. Souri, N.J. Navimipour, Behavioral modeling and formal verification of a resource discovery approach in Grid computing, Expert Syst. Appl. 41 (8) (2014) 3831–3849.
[118] N. Ghadimi, A. Afkousi-Paqaleh, A. Emamhosseini, A PSO-based fuzzy long-term multi-objective optimization approach for placement and parameter setting of UPFC, Arabian J. Sci. Eng. 39 (4) (2014) 2953–2963.
[119] H. Manafi, N. Ghadimi, M. Ojaroudi, P. Farhadi, Optimal placement of distributed generations in radial distribution systems using various PSO and DE algorithms, Elektronika ir Elektrotechnika 19 (10) (2013) 53–57.
[120] M. Mir, M. Kamyab, M.J. Lariche, A. Bemani, A. Baghban, Applying ANFIS-PSO algorithm as a novel accurate approach for prediction of gas density, Pet. Sci. Technol. 36 (12) (2018) 820–826.
[121] I. Ahmadian, O. Abedinia, N. Ghadimi, Fuzzy stochastic long-term model with consideration of uncertainties for deployment of distributed energy resources using interactive honey bee mating optimization, Front. Energy 8 (4) (2014) 412–425.
[122] V. Panahi, N. Jafari Navimipour, Join query optimization in the distributed database system using an artificial bee colony algorithm and genetic operators, Concurr. Comput. Pract. Exp. (2019).
[123] M. Eskandari Nasab, I. Maleksaeedi, M. Mohammadi, N. Ghadimi, A new multiobjective allocator of capacitor banks and distributed generations using a new investigated differential evolution, Complexity 19 (5) (2014) 40–54.
[124] M. Hamian, A. Darvishan, M. Hosseinzadeh, M.J. Lariche, N. Ghadimi, A. Nouri, A framework to expedite joint energy-reserve payment cost minimization using a custom-designed method based on Mixed Integer Genetic Algorithm, Eng. Appl. Artif. Intell. 72 (2018) 203–212.
[125] R. Morsali, N. Ghadimi, M. Karimi, S. Mohajeryami, Solving a novel multiobjective placement problem of recloser and distributed generation sources in simultaneous mode by improved harmony search algorithm, Complexity 21 (1) (2015) 328–339.
[126] N. Razmjooy, F.R. Sheykhahmad, N. Ghadimi, A hybrid neural network–world cup optimization algorithm for melanoma detection, Open Med. 13 (1) (2018) 9–16.
[127] N. Razmjooy, M. Ramezani, N. Ghadimi, Imperialist competitive algorithm-based optimization of neuro-fuzzy system parameters for automatic red-eye removal, Int. J. Fuzzy Syst. 19 (4) (2017) 1144–1156.
[128] M. Habibi, N.J. Navimipour, Multi-objective task scheduling in cloud computing using an imperialist competitive algorithm, Int. J. Adv. Comput. Sci. Appl. 1 (7) (2016) 289–293.
[129] O. Abedinia, N. Amjady, N. Ghadimi, Solar energy forecasting based on hybrid neural network and improved metaheuristic algorithm, Comput. Intell. 34 (1) (2018) 241–260.
[130] M.T. Hagh, H. Ebrahimian, N. Ghadimi, Hybrid intelligent water drop bundled wavelet neural network to solve the islanding detection by inverter-based DG, Front. Energy 9 (1) (2015) 75–90.
[131] H. Aghazadeh, M.B. Germi, B.E. Khiav, N. Ghadimi, Robust placement and tuning of UPFC via a new multiobjective scheme-based fuzzy theory, Complexity 21 (1) (2015) 126–137.
[132] N. Ghadimi, Solar energy forecasting based on hybrid neural network and improved metaheuristic algorithm, Complexity 21 (1) (2015) 78–93.
[133] H. Khodaei, M. Hajiali, A. Darvishan, M. Sepehr, N. Ghadimi, Fuzzy-based heat and power hub models for cost-emission operation of an industrial consumer using compromise programming, Appl. Therm. Eng. 137 (2018) 395–405.
[134] A. Nouri, H. Khodaei, A. Darvishan, S. Sharifian, N. Ghadimi, Optimal performance of fuel cell-CHP-battery based micro-grid under real-time energy management: an epsilon constraint method and fuzzy satisfying approach, Energy 159 (2018) 121–133.
[135] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach, Comput. Commun. 98 (2017) 52–71.

Somaye Hajiheidari received her B.S. in computer engineering, software engineering, from Tabriz Branch, Islamic Azad University, Tabriz, Iran, in 2008; the M.S. in computer engineering, Software engineering, from Tabriz Branch, Islamic Azad University, Tabriz, Iran, in 2016. She is a computer teacher at Ministry of Education, Ajabshir, Iran. Her research interests include Intrusion Detection, Internet of Things, Building Smart Cities, Cloud Computing, and E-Health.

Karzan Wakil is a lecturer and researcher in the Sulaimani polytechnic University, Iraq. He received his BSc degree in Computer Science, College of Science Education from University of Salahaddin. Iraq, 2006. And his M.Sc. degree from the Department of Computer Science in the Faculty of Computing, University Technology Malaysia (UTM). Malaysia, 2013. Currently he is a Ph.D. student in the Department of Software Engineering, Faculty of Engineering, University Technology Malaysia. He is working as a lecturer from 2006 till now, and at the same time, he has served as an ICT Director in University of Human Development. In 2016 he became the head of Science Department in the Institute of Training and Educational Development in Sulaimani, Iraq. Later on, He became a member in some international organizations and communities such as, IEEE, IACSIT, IAENG, and SERG. His research interests are in Web Engineering, Software Engineering, Web Development, Software Development, Web and Software Modeling, Artificial Intelligence, and Information Retrieval and Educational Development. Wakil's experience covers twelve years in the field of computer Science as a lecturer, IT Technician and Developer. He has worked as a lecture in a number of Universties, and Institutions in Sulaymaniyah city of Iraq, such as Sulaimani Polytechnic University, University of Human Development, Garmian University, Sulaimani University, Fine arts Institute, Technical Institute of Sulaimani, Institute of Training and Educational Development, and National Institute of Technology. At the same time, Wakil also worked as an IT Technician and Developers in different Organizations such as, GaliKurdistan TV and Ziba Technology. During his employment served as an ICT Director in the University of Human Development, Head of Department in Institute of Training and Educational Development, and Head of IT department in the National Institute of Technology.

Maryam Badri was graduated from Payame Noor-Garmi University in Ardabil, Iran in 1995. She received the M.S. in telecommunication from Ahar Branch, Islamic Azad University, Ahar, Iran. Her research interests include Social Networks, Internet of Things, and Cloud Computing.

Nima Jafari Navimipour received his B.S. in computer engineering, software engineering, from Tabriz Branch, Islamic Azad University, Tabriz, Iran, in 2007; the M.S. in computer engineering, computer architecture, from Tabriz Branch, Islamic Azad University, Tabriz, Iran, in 2009; the Ph.D. in computer engineering, computer architecture, from Science and Research Branch, Islamic Azad University, Tehran, Iran in 2014. He is an assistance professor in the Department of Computer Engineering at Tabriz Branch, Islamic Azad University, Tabriz, Iran. His research interests include Cloud Computing, Social Networks, Fault-Tolerance Software, QCA, Internet of Things, and Network on Chip.