International Journal of Computers and Applications

ISSN: 1206-212X (Print) 1925-7074 (Online) Journal homepage: http://www.tandfonline.com/loi/tjca20

Swarm intelligence in anomaly detection systems: an overview

Sanju Mishra, Rafid Sagban, Ali Yakoob & Niketa Gandhi

To cite this article: Sanju Mishra, Rafid Sagban, Ali Yakoob & Niketa Gandhi (2018): Swarm intelligence in anomaly detection systems: an overview, International Journal of Computers and Applications, DOI: 10.1080/1206212X.2018.1521895

To link to this article: https://doi.org/10.1080/1206212X.2018.1521895

Published online: 20 Sep 2018.

INTERNATIONAL JOURNAL OF COMPUTERS AND APPLICATIONS
https://doi.org/10.1080/1206212X.2018.1521895

Taylor & Francis
Taylor & Francis Group

Swarm intelligence in anomaly detection systems: an overview

Sanju Mishra [a], Rafid Sagban [b], Ali Yakoob [c] and Niketa Gandhi [d]

[a]Department of Computer Applications, National Institute of Kurukshetra, Haryana, India; [b]Department of Network Information, Faculty of Information Technology, University of Babylon, Babylon, Iraq; [c]Computer Science Department, University of Babylon, Babylon, Iraq; [d]Machine Intelligence Research Labs (MIR Labs), Auburn, WA, USA

ABSTRACT

In an era of the industrial internet of things (IoT), data transferred or saved is always vulnerable to attacks. The IoT networks are needed for implementing security in IoT devices. The IoT networks are considered as secured with authentication and encryption, but these networks are not protected against cyber-attacks. Although there exist hundreds of data protection systems, but there are some shortcomings as well. Thus, anomaly detection takes the responsibility upon itself to make various kinds of attacks less vulnerable. This is achieved by making use of the power of data mining algorithms and tools to analyze and capture any anomalous network traffic. Swarm intelligence has been integrated with data mining to generate lightweight but robust methods to detect and identify the flow of data effectively. This review paper pursues a twofold goal. First is to review various swarm-based anomaly detection methods and to provide new insights in that direction. Secondly, to replenish the literature with fresh reviews on swarm-based data mining studies based on anomaly detection. Further it discusses various methods and architectures of anomaly detection based on statistical, machine learning and data mining techniques.

ARTICLE HISTORY
Received 15 July 2018
Accepted 5 September 2018

KEYWORDS
Anomaly detection; machine learning; statistical anomaly detection; swarm intelligence

Introduction

The internet of things (IoT) is a collection of objects or devices (things) such as sensors, transceivers and actuators that have the ability to collect and analyze data about themselves and their environment to act intelligently to other objects through the internet [1]. IoT can be applied in all aspects of our life for better enjoyment and management. IoT is a heterogeneous network that is more complex than other networks. As it becomes pervasive every day, attacks against it are also increasing. Monitoring such kind of networks is quiet challenging and hard because of the large number of connected devices and the heterogeneity of the exchanged data. Generally, an IoT device gathers sensing data and sends it to a central system for further processing via gateways. Anomalies in data forwarded by IoT devices might be identified at an application layer in the central systems [2]. Minimum attention has been paid to mining data generated by IoT devices themselves. Anomaly-based Intrusion Detection Systems are cyber-attack detection techniques designed to detect intrusions and misuse by capturing system/network activity and classifying it as either normal or anomalous behavior. IDS must have low *false alarm rate* (FAR) with high attack *detection rate* (DR) at the same time. This paper discusses several methodologies and techniques used to reduce the anomalous behavior of networks in IoT systems. There is a need to represent bio-inspired methodologies and techniques to reduce the FAR and increase the DR.

Swarm Intelligence (SI) is a collection of bio-inspired methodologies, techniques and algorithms for complex problem solving. It simulates the collaborative behavior (for example, ants foraging, bee foraging and birds flocking) of some insects, birds and fishes to solve complex tasks like searching food, nest organization, movement synchronization or travelling as a single entity with high speed [3]. The main focus of SI is to design robust systems that can operate intelligently without centralized control [4]. Examples of SI methodologies are ant colony optimization (ACO), particle swarm optimization (PSO) and artificial bee colony (ABC) [5]. Thus, SI-based IDS are more fit to the IoT environment as they are generally lightweight systems to be implemented. This paper has three main contributions for the researchers of this domain.

(1) From the existing literature, 45 papers were studied in detail and summarized in a tabular format for identifying several data sets and ADS.
(2) It is observed that the literature highlights more about the FAR and DR from different research carried out in this domain.
(3) This paper attempts to classify and categorize the literature about this subject. Furthermore, the usage of reviewing SI models discussed and examined in the detection of abnormal data or behavior. This paper is structured as follows. Section 2 discusses the anomaly detection techniques and their categories. Section 3 presents SI-based IDS. Section 4 provided a detailed discussion before the paper is concluded. Finally, conclusion is drawn in Section 5.

CONTACT Sanju Mishra sanju.tiwari.2007@gmail.com

Anomaly detection techniques

The threat of cyber-attacks, crimes and terror is increasing exponentially. After years of research in the area of cyber security, it is well known that the current cyber infrastructure is not efficient enough and thus need many more improvements. This has motivated the development of IDS systems as adaptive defense mechanisms. IDS systems are categorized into three classes, namely signature, anomaly and hybrid detection systems. The first class identifies patterns of traffic supposed to be malicious. The second class compares such patterns to normal baseline and the third class combines techniques from both the techniques [6–8]. This paper focuses on the second class which is anomaly detection systems. Several techniques for anomaly detections are available for detecting insider attacks such as identifying credit card thefts, application fraud and account takeover. An anomaly detection system generates an alert whenever the user performs any action that is beyond the user's normal profile. It detects unknown attacks that are not identified previously through two phases. These are the training phase in which the profile of normal traffic is described and the testing phase in which the profile of learning applied to new data. Several architectures can be found in the literature. These are the statistical, data-mining and machine learning-based techniques [8].

An intrusion detection system has been designed using the Fuzzy Q-learning (FQL) algorithm [9] to protect wireless nodes within the network and target nodes from DDoS attacks to detect the attack patterns and take appropriate countermeasures. A distributed intrusion detection system named Cooperative IDS [10] had been represented to protect wireless nodes within the network and target nodes from DDoS attacks by using a Cooperative Fuzzy Q-learning (Co-FQL) optimization algorithmic technique to identify the attack patterns. A fuzzy theory named FR TRUST has been introduced in a trust overlay network that models the storage of reputation information and network structure. This fuzzy theory is used by the system to estimate a peer trust level, which may be either Low, Medium or High [11]. Several security issues and network attacks are discussed by Javadi et al. [12] addressing service problems of unsolved quality which can produce a serious security issue in WBANs with substantial potential. Various methods and architectures of anomaly detection systems are reviewed and classified in this paper. These include machine learning-based techniques, data-mining-based techniques and statistical-based techniques. Figure 1 depicts the main hierarchy for existing anomaly detection-based IDS. Each of them is discussed in the following section.

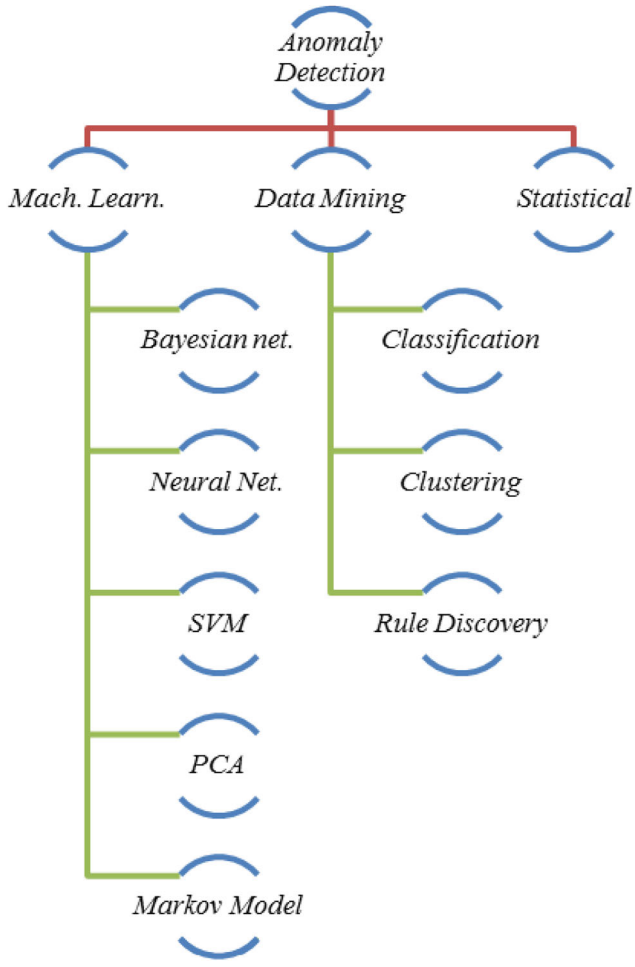

Figure 1. Classification of anomaly detection-based IDs.

Machine learning techniques

The type of systems that enhance their performance based on their previous state are referred as Machine Learning techniques [8]. Feizollah et al. [13] evaluated several machine learning classifiers and they are discussed in the following subsections.

Bayesian networks

A Bayesian network is a directed acyclic graph in which the nodes are associated with probability functions. It is used in the suppression of false alarms and classification tasks within the anomaly detection domain. Speed of the Bayesian network is not high, it will be significant to use when the data set is very large [8].

Neural network

It is a collection of interrelated nodes created to emulate the human brain functions. Each node has a weighted connection to various other nodes in neighboring layers [14]. In the neural network approach, it learns to interpret the nature of the different daemons and users into the intrusion detection system. The prime benefit of neural networks is their strength to uncertain information and unreliable data and their ability to determine the results from data without having previous knowledge of the data regularities.

Support vector machine

Support vector machine (SVM) are a group of related supervised learning tasks used for regression and classification [15]. It is mostly used in the pattern recognition field and also used in anomaly detection systems. The one class SVM is based on one example set belonging to a specific class and positive example, rather than using both negative and positive example. When compared to neural networks in the KDD cup data set, it was

noticed that SVM out performed Neural Network in terms of accuracy and FAR in several types of attack [16].

Principal components analysis

A technique called principal component analysis (PCA) [17] is introduced for facing the problem of high-dimensional data sets. PCA is useful in several domains such as pattern recognition, anomaly detection and image compression. For example, the anomaly detection scheme was introduced by Shyu et al. [18] in which the dimensionality of the audit data is reduced.

Markov models

Markov chains have also been applied for anomaly detection. For example, in the study of Ye et al. [19], the normal activities of a network system are represented by a Markov-chain model of heuristic data. Such kind of data was analyzed to infer the probability of supporting the normal activities. An example of how the Markov chain is generated can be depicted by two colored die, each one referring to one of two system states: normal or abnormal. The probability of transmitting from the current state to the next state is depicted by a colored ball chosen from a bag. Another Markov-chain technique is called the Hidden Markov model (HMM) in which some of the system states are hidden from the user.

Data mining techniques

Data mining techniques are applied to anomaly-based IDS with an aim of building a predictive or perspective model from the network under monitoring. The applications of data mining in anomaly detection and its future scope were reviewed by Mukhopadhyay et al. [20]. Several data mining approaches can be found in the literature, they are classification-based, clustering-based and rule-based discovery.

Classification-based approach

The classification-based anomaly detection system is considered as a system that has the ability to identify the data as anomalous or normal [21]. The process of classification commonly includes several steps:

(1) Analyze classes and class attributes from training data.
(2) Analyze attributes.
(3) Use the training data to learn the model.
(4) Apply the learned model to distribute the unknown data samples.

To accomplish the above steps several techniques for classification are introduced such as fuzzy logic, inductive rule generation techniques and genetic algorithms.

Outlier detection/clustering-based approach

The patterns in unlabeled data with several dimensions can be identified using the clustering-based approach [22]. Clustering algorithms are efficient to diagnose anomalies without prior knowledge. Outlier Detection and Clustering are jointly related. From the perspective of anomaly detection, the objects that are not placed in the clusters of a data set can be represented as attacks/intrusions.

Rule-based discovery approach

In data mining, the events that tend to exist together can be expressed using the rule-based discovery association approach [23]. Two important concepts are rule support and rule confidence to deal with the association rules. The rules are used to mine collected traffic data to obtain normal patterns for anomaly detection. They are also used to design an anomalous connections summary identified by the IDs.

Statistical techniques

The system can monitor its activities to initiate profiles and exhibit their behavior. The profile generally involves measures such as audit record distribution measure, categorical measures, activity intensity measure and ordinal measure [24]. Mostly, two profiles are managed for each subject: the stored and the current profile. As the network events are processed, the IDS notifies the degree of inconsistencies for the particular event as an anomaly by comparing the stored profile with the current profile using an abnormality function of all measures within the profile. An alert is generated by the intrusion detection system, if the anomaly score is greater than a certain threshold.

In statistical approaches, the anomaly detection scheme does not need prior knowledge of attacks or flaws. Statistical approaches can provide accurate notification of malicious activities that are generally recognized over extended duration and are best indicators of impending denial-of-service (DoS) attacks. Ports scan is a common example of such an activity. Generally, the distribution of ports, scan is greatly anomalous in comparison to the normal distribution of traffic. An enhanced version of IDES termed as the Next-Generation Intrusion Detection Expert System (NIDES) [25] was considered as real time IDS for constant monitoring of user activity or could run in a batch mode for periodic analysis of the audit data.

Swarm intelligence algorithms in IDS

The term 'Swarm Intelligence' was firstly triggered by Beni et al. [26] in context of the 'intelligent' behavior in the cellular robotics system. Later on, the term transformed into mature research field of methodologies, techniques and algorithms for problem solving in artificial intelligence. SI methodologies draw their inspiration from the behavior of birds, insects and fishes, and their ability to work as a group of agents. Indeed, the individual intelligence of such social agents is limited. However, when they socially connect with each other or with their environment they seem to be able to perform difficult tasks without the presence of a centralized authority (for example, the queen of the colony). Because of the maturation, simplicity, robustness and adaptively of SI algorithms, they have been successfully applied in anomaly detection.

Ant colony optimization

ACO is a meta-heuristic to solve optimization problems simulating the behaviors of ant colonies in biology such as the food foraging behavior [27]. Ants swarm is being able to continually locate the shortest way from their nest to the food. Ants lay a chemical substance called *Pheromone* into the ground through

their trip searching for food [28]. Laid pheromone will attract forager ants to follow the same trip paths. The other ants find and move to the location with the chemical substance, ants will tend to move along the path instead of moving in a random pattern. After some time, in some paths, the chemical substance or pheromone will evaporate which results in the reduction of attracting the ants and then they find and move to the position with pheromone which is more likely to strengthen the attraction. At the end of the path, the ants with poor performance will disappear. ACO meta-heuristic transformed this natural optimization into a computational optimization process for problem solving.

Feature selection is one of the optimization problems that IDS suffer from. ACO is one of the nominated techniques to solve such kind of problems because of its simplicity and quick convergence. Aghdam and Kabiri [29] designed a new heuristic function based on the length of the selected feature vector. In spite of using ACO to speed up the convergence, the proposed model used the Ant System variant model which is not one of the best ACO models such as the Max-Min Ant System.

The ACO-based clustering method is used to detect the outliers [7], it performs a data preprocessing that leads to detect the outliers. Each ant compares the property value with the initial point set and checks data points importance and updates the values of the pheromones of other ants. Finally, the data points are selected and the final clustering matrix is obtained. All the remaining data points (unselected) are considered as outlier. ACO-based clustering have an acceptable correctness rate without initializing the centers and the number of clusters.

Hamamoto et al. [30] proposed a hybrid signature-based theme of anomaly detection. Hybridization was between the genetic algorithm (GA) and ACO models. To predict the network behavior of a given day, data of previous days are collected and Denial of Service (DoS) and Distributed DoS (DDoS) attacks are used in simulation. This way of flow analysis recurred in [6] between ACO and PCA, the statistical procedure. There is great potential of using other machine learning procedures with ACO such as the decision trees and random forests [31]. Unfortunately, most of the yet reviewed ACO-based IDs omitted the global framework of the searching algorithm except ACSMiner [32] which took into account the impact of using effective updating pheromone in IDS performance.

Particle swarm optimization

The model of PSO, developed by Eberhart and Kennedy in 1995 [33], is based on the social behavior of fish flocking and bird schooling in their coordinated movement dynamics [33]. The synchronization of such group behavior was made by the birds to maintain optimal distance between themselves and their neighbors. There are three basic rules to control this natural optimization process. These are *Collision Prevention*, *Speed Adjustment* and *Herd Centering*. The first rule is to avoid neighbors by readjusting their physical position. The second rule is to synchronize their speed with their neighbors. The third rule is to stay close to their herd mates. Several PSO applications in the field of anomaly detection can be recognized.

Lima et al. [7] presented the signature-based approach to profile the normal network traffic behavior in real traffic environment. Because of the powerful characteristics of PSO, for example its low computational complexity, ability to escape from local optima and small number of input parameters, it was integrated to achieve high convergence rate. Poornian et al. [6] represented a new optimized scheduling hybrid algorithm named as GPSO. It is a combination of Gel algorithms and PSO.

Artificial bee colony

ABC simulates behavior of real bees and contains three groups of bees for solving multimodal optimization and multidimensional problems [34]. The three groups are onlookers, scouts and employed bees. The behavior of honey bees can be categorized in terms of their responsibility and the work that they carry. The bee is called as an onlooker if they are waiting on the dance area for making decision to choose a food source; if the bee revisited the pervious food source it is named as an employed bee; and a scout bee where individual bees search randomly without prior information for the location of food.

In the ABC algorithm, the roles of employed bees, onlookers and scout are interchangeable among the individuals; an employed bee's job is to mine and gather the required information, while scouts exploit for new food sources, whereas onlookers are in charge of sharing information with scouts and employed bees by communicating in the dance area.

Firefly algorithm

The firefly algorithm (FA) is problem solving method developed by Yang and He [35] for the mathematical optimization and engineering problems inspired by the flashing behavior of some insects called fireflies. Flashing behavior is producing rhythmic flashes through a process called bioluminescence which is a way of direct communication to attract the prey and for defense from predators. This intensity of light will guide the swarm of fireflies toward their colleagues. Intensity of light is inversely proportional to the distance from the light source. In FA [36], there are three idealized rules which are the attractiveness regardless of the gender, the attractiveness of high bright insects to the lower bright ones and the objective function that simulates that brightness. The FA are powerful and with distinct techniques in the optimization of an objective function, especially for a wide search space. The two models used the flow data in its anomaly detection task. Good results have been gained with real world data iwhich is the backbone of a university.

Cuckoo search optimization

Cuckoo search is a heuristic search algorithm [37]. This algorithm operates based on the reproduction strategy of a bird called the cuckoo. This cuckoo bird does not create a nest for itself; therefore, it uses the nests of other birds to lay their own eggs. This cuckoo bird has an ability to lay eggs just like the egg of the host bird. It is one of the reinforcement in the cuckoo bird. If the host bird discovers the eggs that are not hers, it disposes the nest and it creates a new nest in some other places. The

eggs' size is bigger when compared with the host's bird until the cuckoo bird would hatch. Every cuckoo cares about his nest.

CSO and K-means [38,39] clustering is used as an anomaly detection technique that performs two phases, namely that are the training phase and the detection phase. Mean square error and Silhouette Index methods are applied in as multi-objective functions to evaluate the anomaly detection measure and the classification measure.

Discussion

Several SI-based anomaly detection IDs are successfully applied. This section summarizes this success through drawing certain conclusions. Table 1 presents a conceptual comparison of some of the previous review papers in the period (2011–2018). The main goal of this summary is to highlight the uncovered subjects in cyber security literature.

Table 1. Summary of similar review papers.

Review paper	Year	Index of publication	Evolved paradigms	Application domain	ID phase	Notes related to SI and/or anomaly-based IDs
[40]	2011	_Scopus _Science Citation Index Expanded (SCIE)	_Swarm Int.	IDS	Any phase	_SI-based IDS fail to take advantage of the full potential of ACO for classification _PSO-based IDS have been studied more than ACO-based ones in combination with other ML techniques _it seems that SI-based IDS did not benefit from the simplicity and distribution characteristics of ACO in designing fast and distributed IDS
[41]	2012	_Google Scholar	_Swarm Int.	IDS	Any phase	__ only focused on only two SI techniques: ACO & PSO
[42]	2014	_Scopus _Emerging Sources Citation Index (ESCI)	Any	cyber security systems	Any phase	_short conclusion _general description without reviewing the literature
[43]	2015	_EBSCO _Google Scholar	_Evolutionary Comp. _Swarm Int. _Parallel comp._Mach. Learn._Graph DB _Big Data analytics	IDS	Any phase	_short conclusion _small number of reviewed SI papers _low publication index
[44]	2015	_EBSCO _Google Scholar_Scopus _Emerging Sources Citation Index (ESCI)	_Evolutionary Comp. _Swarm Int.	IDS	Any phase	_little interest in literature on parameter adaptation in SI-based IDS _little interest in literature on cloud computing and big data analytics in SI-based IDS _an absence of metrics/ frameworks for evaluating IDS _mainly focused on ACO & PSO
[45]	2015	_Google Scholar_Scopus _Emerging Sources Citation Index (ESCI)	_Swarm Int.	Outlier detection	data exploring	_mainly focused on ACO, BCO & PSO
[46]	2016	_Scopus _Science Citation Index Expanded (SCIE)	_Evolutionary Comp. _Swarm Int. _Mach. Learn.	IDS	Any phase	_mainly focused on GA and GP and ignored SI-based IDS that standalone or hybridized with machine learning
[16]	2016	_Scopus _Science Citation Index Expanded (SCIE)	_Mach. Learn.	Anomaly detection	Any phase	_totally ignored SI-based IDS hybridized with machine learning
[47]	2016	_Scopus	Any	Anomaly detection	Any phase	_totally ignored SI-based IDS hybridized with machine learning
[14]	2017	_Google Scholar _Scopus	_Swarm Int.	IDS	data classification	__ only focused on only two SI techniques: BA & PSO
[48]	2018	_Scopus _Science Citation Index Expanded (SCIE)	_Bio-Inspired Algorithms	cyber security systems	data clustering data classification	__ little focused on SI techniques ACO & PSO _an absence of anomaly-based detection using SI
[49]	2018	_Scopus _Science Citation Index Expanded (SCIE)	_hybrid algorithm	IDS	Any Phase	- data filtered using the Vote algorithm for feature reduction

Table 1 includes the publishing index, involved paradigm and application domain, the phase of intrusion detection and strengths or weaknesses of the work carried out by other researchers. Several online databases, especially those that are indexed in Google Scholar, Scopus, ESCI and SCIE have listed this work performed by other researchers.

Figure 2 shows the distribution of publications in this domain by online databases which clearly indicate that the growth rate in SCIE publications is the highest and Scopus is the lowest in the last eight years compared to other databases. It is obvious that most of covered subjects are about how the SI-based methods are applied in IDS in general. The involved methodologies that are discussed in such existing works were distributed on evolutionary computing, swarm intelligence, parallel computing, machine learning, graph database and big data analytics. Any methodology is applied according to the cyberspace for which it was designed. Four cyberspace domains are covered by these review papers: they are Intrusion Detection, Cyber-security, Outlier Detection and Anomaly detection as depicted in Figure 3. This figure clearly shows that intrusion detection and cyber security are covered by all the methodologies and anomaly detection techniques.

Table 1 contains the ID phase for which the perspective architecture was designed. For example, swarm intelligence and bio-inspired methods applied for data exploring phase are reviewed in [45] and for the data classification phase in [14,48], respectively. It can be witnessed that in all given cases, the SI architecture can be applied for all phases and any application domain of cyber-security. This confirms that the role of SI in preventing network attacks has been explored for ID in general rather than explored for specific ID phase or ID application domain. One can notice that the previous review work focused two or three SI models and neglected the potential role of other models. This review paper has benefited from such drawbacks as shown in Table 2 which summarizes swarm-based methods in Anomaly Detection.

Table 2 consists the following entries: name of the SI method, the diversity mechanism utilized to guide the search, data set used in verification, the type of attack, the performance metrics and the limitations in each applied SI method. From the first entry one can notice that ACO is widely integrated with the IDS architecture as shown in Figure 4. The diversity mechanism entry shows clearly that most of the existing work rely on hybridization either with standard anomaly detection techniques as in references [7,50,52] or with other SI models as in references [51,56].

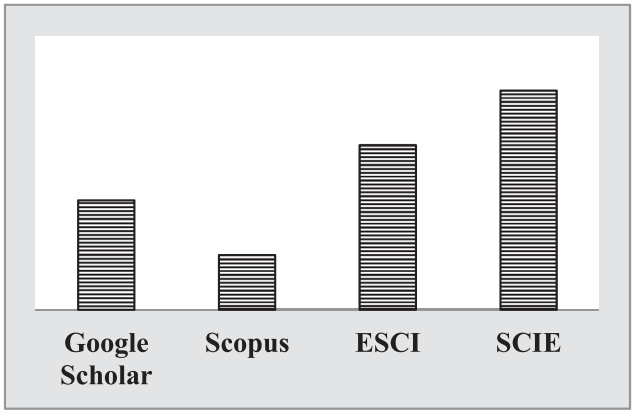

Figure 2. The distribution of review papers according to their index of publications (2011–2018).

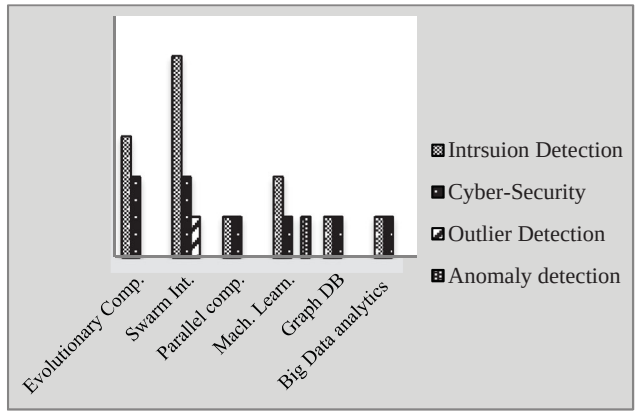

Figure 3. The distribution of review papers according to their involved paradigm (2011–2018).

Thus, diversity-wise proposals should be contributed in the future to address this gap as the exploration and exploitation trade-off is critical in the design of such search methods. Fewer attacks and data sets, on the other hand, are seen in the experimental design of existing SI-based IDS. For the data sets part, NSL-KDD was in the background. This may produce one-sided vision about collected data and not reflect real world situations. For the attacks' part, Figure 5 shows that DoS, U2R, Probe and R2L are highly tackled attacks among all cases and DDoS is the lowest.

Conclusion

The IoT environment requires lightweight anomaly-based IDS for their security. This paper focuses on the application of the SI technique in anomaly detection as they are the simple yet algorithms for this purpose. A comprehensive conceptual analysis of the methods that perform effective anomaly detection is presented. The paper highlights the neglected aspects that other studies have not covered to the best of our knowledge. Analysis of these methods, along with tabulations of their specific working models, performance metrics, efficiency, robustness, diversity of search and accuracy levels are discussed in detail. This review comes out with several conclusions. Firstly, there are many aspects of SI-based techniques that remain unexplored. Secondly, existing SI-based anomaly detection solutions failed to take advantage of the full potential of SI for the detection. Thirdly, PSO-oriented approaches were extensively studied compared with ACO and other recently established SI models. Fourthly, more awareness should be taken to activate the role of diversity of search to provide excellent DRs.

Disclosure statement

No potential conflict of interest was reported by the authors.

Table 2. Summary of swarm-based anomaly detection techniques.

Ref.	Year	The name of SI tech.	Diversity tech.	Data set	Type of attack	Efficiency: high DR & low FAR	Objs/limits
[7]	2010	PSO	_hybridizing with k-means	Real collected data	NA	DR = 99.13, FAR = 5.02	_ type of attacks did not determined _comparisons: no
[50]	2012	FA	_hybridizing with k-means	Real collected data	NA	FPR = 20% TPR = 80%	_ less efficient than the rate achieved by other methods
[51]	2015	ABC + PSO	_hybridizing two global search methods	KDDCup'99	DoS, U2R, Probe, R2L,	DR = 98.67	_comparisons: yes _objs: select traffic features to predict the ID problem
[52]	2015	PSO	__ apply PSO to tuning the parameters of MCLP model	KDD CUP 99	DoS, U2R, Probe, R2L,	DR = 99.13, FAR = 1.947	_comparisons: yes _obs: to improve the efficiency of attack detection
[30]	2015	ACO	Generating a near-optimal characterization for networks using GA and DSNSF	Real collected data	DoS and DDoS	Correlation Coefficient and Normalized Square Mean Error	_uses a signature-based ID methodology which is different from the theme of anomaly detection
[53]	2015	FA	Introduced Firefly Algorithm(FA) and GA to detect network anomalies	Data collected from a university	DoS and DDoS	TPR of FA = 77.4% FPR of FA = 0.4%	_yes both models had a great performance with a minimum detection of false alarms
[29]	2016	ACO	_ the length of selected feature vector used as a heuristic function and performance metrics	KDD Cup 99 and NSL-KDD	DoS, U2R, Probe, R2L,	DR = 98, FAR = 1	_comparisons: yes _obs: to identify important features in building an intrusion detection system _in spite of using ACO to speed up the convergence, the proposed model used Ant System variant model which is not one of the best ACO models
[54]	2016	PSO	Proposed an ID framework based on time-varying chaos PSO combined with MCLP and SVM	NSL-KDD	DoS, Probe, U2R, and R2L,	DR = 97.23 FAR = 2.41	_yes Compared with other existing model and claimed for better performance than others.
[6]	2016	ACO	Creating a model which characterize the normal traffic behavior called DSNSF	Real collected data	DDoS and Flash Crowds	TPR = 92% FPR = 21% For ACODS FPR = 24%	_yes Compared the result of PCADS with ACODS and PCADS performed better than ACODS
[31]	2017	ACO	Proposed a new developed Ant Tree miner (ATM) method for intrusion detection	The NSL-KDD data set	Probe, U2R, R2L, Dos	ACC. = 78% Low FAR, with DR over 90%	Yes Compared with J48, Random Tree, SVM and M-Layer Perceptron.
[55]	2017	CS	Proposed a robust anomaly detection technique, Fuzzified Cuckoo-based Clustering Technique (F-CBCT)	The NSL-KDD	DoS, Probe U2R R2L	DR = 96.86%, FPR = 1.297%	_Yes compared with the other state-of-the-art techniques
[56]	2018	ABC + Other SI	propose a new hybrid classification method based on ABC and AFS. The FCM and CFS techniques to divide the training data set.	NSL-KDD and UNSW-NB15	DoS, U2R, Probe, R2L	DR = 99%FPR = 0.01% 99%	_yes comparing the proposed method with other state-of-the-art techniques

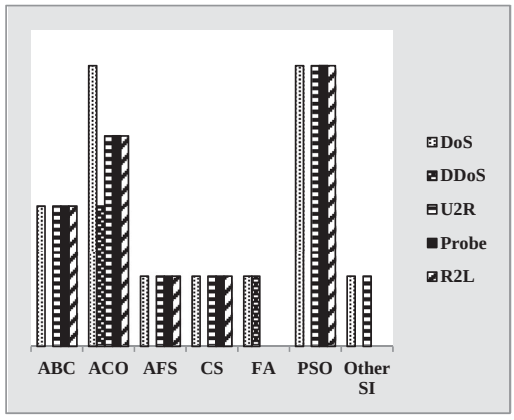

Figure 4. Types of involved attacks (2010–2018).

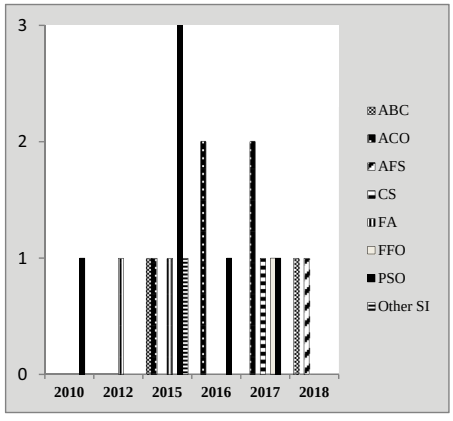

Figure 5. The distribution of the SI-based IDS in the period (2010–2018).

Notes on contributors

Sanju Mishra is a Research Associate for a sponsored research project "Intelligent Real time Situation Awareness and Decision Support System for Indian Defence" funded by DRDO in Department of Computer Applications, National Institute of Technology, Kurukshetra. Her current research interests include Knowledge Based Systems, Intelligent Decision Support, Semantic/Intelligent Query Search Engines, Intrusion Detection, Swarm Intelligence. She has to-date published 19 research papers one 1 book chapter with international and national publishers. She is the member of IEEE. She is working as an organizing committee member for the conferences of MIR Labs, USA. She is the Guest Editor for IGI-Global and Inderscience Journals.

Dr. Rafid Sagban holds a Bachelor in computer sciences from university of babylon, Babil, Iraq in 2001 and Higher Diploma in data security from iraqi commission for computers & informatics - informatics institute for postgraduate studies in 2002, Baghdad, Iraq. His Master's degree and Ph.D in information technology are both from northern university of malaysia, Sintok, Malaysia in 2011 and 2015 respectively. Rafid's research and development experience includes over 15 years in the Academia and Industry. He works in a multi-disciplinary environment involving algorithm analysis, swarm intelligence, business intelligence, internetworking, and web graphics and optimization. He is currently member of Machine Intelligence Research Labs, USA; member of Iraqi Association for IT Specialists, Iraq; member of IEEE Computational Intelligence Society/IEEE Malaysia Section, Malaysia; and reviewer/editor of several international academic journals and conferences.

Dr. Ali Yakoob holds a Bachelor in Computer Sciences from University of Babylon, Iraq in 2001 and Master's degree and Ph.D in Computer Sciences are both from University of Babylon, Iraq in 2005 and 2016 respectively. Ali's research and development experience includes over 6 years in the Academia and Industry. His specialist related to computational intelligence, swarm intelligence algorithms, machine learning, speech processing, and business intelligence.

Dr. Niketa Gandhi is a Senior Member IEEE and has more than 15 years of experience in academics performing various roles in teaching, administration, and research at college and university level. She received her Ph.D. in Computer Science from the University of Mumbai and she has her Bachelor and Master of Science along with Master of Philosophy in Computer Science as well from India. She is currently a Technical Manager at Machine Intelligence Research Labs (MIR Labs), USA. Her primary research relates to area of eAgriculture, use of ICT to improve the production and sustainability of agricultural industry, use of geospatial and data mining techniques to interrogate climate, land use, soil and economic data to create decision support systems for agricultural stakeholders. She is also interested in mining scientific datasets in domains such as healthcare, cyber security, social network, business, demographic, sustainability and intelligence analysis. Her result has resulted in publishing many journal articles, conference papers and posters. She is actively involved in organizing various International conferences supported by IEEE and Springer where she has served as session chair, publication chair and editor of the conference proceedings. She is also a technical program committee member of various International conferences around the world. She is also on the editorial board of many journals and member of professional bodies. She has also been invited as a speaker for various workshops and seminars.

ORCID

Sanju Mishra http://orcid.org/0000-0001-7197-0766
Rafid Sagban http://orcid.org/0000-0002-3518-1396
Ali Yakoob http://orcid.org/0000-0002-9135-8627
Niketa Gandhi http://orcid.org/0000-0002-1745-3036

References

[1] Medagliani P, Leguay J, Andrzej Duda, et al. Internet of things applications - from research and innovation to market deployment. In: Vermesan O, Friess P, editors. Internet of things applications - from research and innovation to market deployment, bringing IP to low-power smart objects: The smart parking case in the CALIPSO project. Series in Communications. Gistrup: The River Publishers; 2014. p. 287–313.
[2] Alghuried A. A model for anomalies detection in internet of things (IoT) using inverse weight clustering and decision tree [Unpublished MSc dissertation]. Dublin Institute of Technology; 2017.
[3] Dorigo M, Birattari M, Stützle T. Ant colony optimization: artificial ants as a computational intelligence technique. IEEE Comput Intell Mag. 2006;1(4):28–39.
[4] Bonabeau E, Dorigo M, Theraulaz G. Swarm intelligence: from natural to artificial systems. New York: Oxford University Press; 1999.
[5] Merkle D, Middendorf M. Swarm intelligence. In: EK Burke, G Kendall, editors. Search Methodologies. Boston (MA): Springer; 2005. p. 317–339.
[6] Fernandes G, Carvalho LF, Rodrigues JJPC, et al. Network anomaly detection using IP flows with Principal Component Analysis and Ant Colony Optimization. J Netw Comput Appl. 2016;64:1–11.

[7] Lima MF, Sampaio LDH, Zarpelão BB, et al. Networking anomaly detection using DSNS and particle swarm optimization with re-clustering. GLOBECOM – IEEE Glob Telecommun Conf. 2010: 1–6.
[8] Patcha A, Park JM. An overview of anomaly detection techniques: existing solutions and latest technological trends. Comput Networks. 2007;51(12):3448–3470.
[9] Shamshirband S, Anuar NB, Laiha M, et al. Anomaly detection using fuzzy Q-learning algorithm. Acta Polytechnica Hungarica. 2014;11(8):5–28.
[10] Shamshirband S, Daghighi B, Anuar NB, et al. Co-FQL: anomaly detection using cooperative fuzzy Q-learning in network. J Intelligent Fuzzy Syst. 2015;28(3):1345–1357.
[11] Javanmardi S, Shojafar M, Shariatmadari S, et al. FR TRUST: a fuzzy reputation based model for trust management in semantic P2P grids. Int J Grid Utility Comput. 2015;6(1):57–66.
[12] Al-Janabi S, Al-Shourbaji I, Shojafar M, et al. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Inform J. 2016;18:113–122.
[13] Ali Feizollah SS, Anuar NB, Salleh R, et al. A study of machine learning classifiers for anomaly-based mobile botnet detection. Malaysian J Comput Sci. 2014;26(4):251–265.
[14] Enache A-C, Sgarciu V, Togan M. Comparative study on feature selection methods rooted in swarm intelligence for intrusion detection. Proceedings – 2017 21st International Conference on Control Systems and Computing. CSCS 2017; 2017.
[15] Sarasamma ST, Zhu QA, Huff J. Hierarchical Kohonenen Net for anomaly detection in network security. IEEE Trans Syst Man Cybern Part B Cybern. 2005;35(2):302–312.
[16] Agrawal S, Agrawal J. Survey on anomaly detection using data mining techniques. Procedia – Procedia Comput Sci. 2015;60:708–713.
[17] Jolliffe I. Principal component analysis. In: Everitt B, Howell D, editors. Encyclopedia of statistics in behavioral science. Hoboken (NJ): John Wiley & Sons, Ltd; 2005. p. 1580–1584.
[18] Shyu ML, Chen SC, Sarinnapakorn K, et al. A novel anomaly detection scheme based on principal component classifier. 3rd IEEE International Conference on Data Mining; p. 353–365; 2003.
[19] Ye N, Zhang Y, Borror CM. Robustness of the Markov-chain model for cyber-attack detection. IEEE Trans Reliab. 2004;53(1): 116–123.
[20] Mukhopadhyay A, Maulik U, Bandyopadhyay S, et al. A survey of multiobjective evolutionary algorithms for data mining: part I. IEEE Trans Evol Comput. 2014;18(1):4–19.
[21] Steinwart I, Hush D, Scovel C. A classification framework for anomaly detection. J Mach Learn Res. 2005;6:211–232.
[22] Guo F, Yang Y, Duan L. Anomaly detection by clustering in the network. Proceedings – 2009 International Conference on Computational Intelligence and Software Engineering. CiSE 2009; 2009.
[23] Hipp J, Güntzer U, Nakhaeizadeh G. Algorithms for association rule mining – a general survey and comparison. ACM SIGKDD Explor Newsl. 2000;2(1):58–64.
[24] Om H, Hazra T. Statistical techniques in anomaly intrusion detection system. Int J Adv Eng Technol. 2012;5(1):387–398.
[25] Anderson D, Frivold T, Valdes A. Next-generation intrusion detection expert system (NIDES): a summary. SRI Int. Menlo Park (CA): SRI International Computer Science Laboratory; May 1995. Report number SRI-CSL-95-07. p. 47.
[26] Beni G, Wang J, Wang J, et al. Swarm Intelligence in Cellular Robotic Systems. NATO Adv Workshop Robots Biol Syst. 1989;102(2):703–712.
[27] Dorigo M, Stützle T. Ant colony optimization. Encycl Mach Learn. May, 2009;1:28–39.
[28] Dorigo M, Bonabeau E, Theraulaz G. Ant algorithms and stigmergy. Futur Gener Comput Syst. Jun. 2000;16(8):851–871.
[29] Aghdam MH, Kabiri P. Feature selection for intrusion detection system using ant colony optimization. Int J Netw Secur. 2016;18(3):420–432.
[30] Hamamoto AH, Carvalho LF, Proenc ML. ACO and GA metaheuristics for anomaly detection. Proceedings - International Conference of the Chilean Computer Science Society, SCCC. 2016. Available from: https://doi.org/10.1109/SCCC.2015.7416569
[31] Botes FH, Leneen L, La Harpe RD. Ant colony induced decision trees for intrusion detection. Proceedings of the 16th European Conference on Cyber Warfare and Security, 2017.
[32] Shen Y, Zheng K, Wu C. Research on intrusion detection based on improved antminer algorithm. Proceedings of Science: International Conference on Information Science and Cloud Computing, Guangzhou, China, 2017.
[33] Kennedy J, Eberhart R. Particle swarm optimization. Proceedings of ICNN'95 – International Conference on Neural Networks. 1995;4:1942–1948.
[34] Karaboga D. An idea based on honey bee swarm for numerical optimization. Erciyes University, Engineering Faculty, Computer Engineering Department; 2005.
[35] Yang XS, He X. Firefly algorithm: recent advances and applications. Int J Swarm Intell. 2013;1(1):36–50.
[36] Fister I, Yang XS, Brest J. Modified firefly algorithm using quaternion representation. Expert Syst Appl. 2013;40(18):7220–7230.
[37] Gariga KR, Reddy ARM, Rao NS. PDA-CS: Profile distance assessment-centric cuckoo search for anomaly-based intrusion detection in high-speed networks. In: Satapathy S, Bhateja V, Udgata S, et al., editors. Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications. Advances in Intelligent Systems and Computing, Vol. 515; 2017.
[38] Jayanthi P, et al. An enhanced cuckoo search approach for outlier detection with imperfect data labels. Int J Adv Eng Technol. June, 2016;7(2):667–673.
[39] Garg S, Batra S. Fuzzified cuckoo based clustering technique for network anomaly detection. Comput Electr Eng. 2017; 1–20.
[40] Kolias C, Kambourakis G, Maragoudakis M. Swarm intelligence in intrusion detection: a survey. Comput Secur. 2011;30(8):625–642.
[41] Amudha P, Rauf HA. A study on swarm intelligence techniques in intrusion detection. Proceedings of International Conference on Research Trends in Computer Technologies (ICRTCT - 2013). 2012. p. 32–34.
[42] Raiyn J. A survey of cyber attack detection strategies. Int J Secur Appl. 2014;8(1):247–256.
[43] Aaron SJS, Balasubramanian R. A Comprehensive Survey of Technologies for Building a Hybrid High Performance Intrusion Detection System. Int J. 2015;113(15):33–40.
[44] Elsayed SM, Sarker R, Essam D, et al. Survey of uses of evolutionary computation algorithms and swarm intelligence for network intrusion detection 2nd reading. Int J Comput Intell Appl. Dec. 2015;14:1550025.
[45] Liu B, Cai M, Yu J. Swarm Intelligence and its Application in Abnormal Data Detection. Informatica. 2015;39(2015):63–69.
[46] Buczak A, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutorials. 2015;18(2):1153–1176.
[47] Bhaya WS, Alasadi SA. Anomaly detection in network traffic using stream data mining: review. Res J Appl Sci. 2016;11(10):1076–1082.
[48] Rauf U. A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions. Arab J Sci Eng. 2018; In Press. https://doi.org/10.1007/s13369-018-3117-2
[49] Aljawarneh S, Aldwairi M, Yassein MB. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J Comput Sci. DOI:10.1016/j.jocs.2017.03.006, 2018
[50] Adaniya MHAC, Lima MF, Rodrigues JJPC, et al. Anomaly detection using DSNS and Firefly Harmonic Clustering Algorithm. IEEE Int Conf Commun. 2012: 1183–1187. DOI:10.1109/ICC.2012.6364088
[51] Amudha P, Karthik S, Sivakumari S. A hybrid swarm intelligence algorithm for intrusion detection using significant features. Sci World J. 2015;2015(1):1–15.
[52] Bamakan SMH, Amiri B, Mirzabagheri M, et al. A new intrusion detection approach using PSO based multiple criteria linear programming. Procedia Comput Sci. 2015;55(Itqm):231–237.
[53] Salmen F, Galego Hernandes PR, Carvalho LF, et al. Using firefly and genetic metaheuristics for anomaly detection based on

network flows. AICT 2015, Eleventh Advanced International Conference on Telecommunications; no. c, p. 113–118, 2015.

[54] Mojtaba S, Bamakan H, Yingjie T, et al. An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization. Neurocomputing. 2016;199:90–101.

[55] Garg S, Batra S. Fuzzified Cuckoo based Clustering Technique for Network Anomaly Detection R. Comput Electr Eng. 2017;0: 1–20.

[56] Hajisalem V, Babaie S. A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. Comput Netw. 2018;136:37–50.