Journal of Good Governance and Sustainable Development in Africa (JGGSDA), Vol. 9, No 4, 2026. Available online at http://journals.rcmss.com/index.php/jggsda. Covered in Scopedatabase-https://sdbindex.com/Sourceid/00000431, google scholar, etc. ISSN: 2346-724X (P) 2354-158X (E)
Bello Ayuba & Muhammad Saidu Aliero, 2026, 9(6):1-13

Review of Intrusion Detection System in Soft-Computing

Bello Ayuba[1], **Muhammad Saidu Aliero**[2]
[1]Department of Computer Science, Federal Polytechnic Idah, Kogi State, Nigeria
[2]Department of Information and Communication Technology, Kebbi State University of Science and Technology, Aliero, Nigeria

Abstract
Historically, data has been collected and processed manually. In recent years, rising from the advent of the international network, millions of computers are connected together for communication purposes. However, it is greatly prone with security challenges. Interestingly, the network system has given an opportunity to monitor and facilitate the solution (or prevention or detection) of problems over the network. This review concludes that there is need for an improved intrusion detection system (IDS) that will provide adequate security measures in real-time. This review focuses on the methodologies of soft-computing in tackling challenges of intrusion detection system. In addition, we draw out the recommendation of other methods applicable to IDS. A lot of studies have been conducted, but they are haphazard. The current authors made attempt to collect this information together to give room for further research and discussions.

Keywords: *Intrusion detection system, network security, soft-computing*

1. Introduction

Today as we attempt to find answers to some real-world problems, however we come to realize that such problems are typically ill-defined problems, difficult to model and with large-scale solution spaces. In such manner, precise models are impractical, too expensive, or non-existent. The applicable available information is in form of empirical prior knowledge and input-output data representing instances of the problem's behavior. To solve such problem, we need approximate reasoning systems capable of handling such imperfect information.

Thanks to the soft Computing technologies which provide us with a set of flexible computing tools to perform these approximate reasoning and search tasks. Today many of the industries and academia counterattack threat and attacks in order to secure computer networks [1, 2].

The rapid growths in evolving computer network, leads to the need of security requirements in computer network. This is because many operating systems and applications are full of security vulnerabilities at many levels [3, 4]. Recent studies reveal that over 63% of web applications are at risk of being compromise due to lack of security prevention measures [5]. One of the prevention measures to secure systems and applications over networks is to deploy intrusion detection system (IDS). Intrusion detections systems are tools that continuously and dynamically monitor behaviours of the systems, they are subjected to observe violation on such systems (usually as second line of defence) [6].

Researchers from academia and industries have provided different IDS scheme and development approaches in soft computing ranging from artificial neural networks to meta-heuristics and evolutionary computing in order to eliminate violation or abuse of security policy, or unexpected behaviours in systems and applications by insider or outsider. Furthermore, recent studies promised ultimate security measures on their proposed system yet in 2014 the world recorded devastating attacks [4,5].

Existing literature [10, 11, and 12] attempt to justify reason for difficulty to eliminate absence of the attacks completely on computer network by focuses general IDS. However, this study is unique by focusing IDS application in soft computing with aimed to identify major issues associated with each approach. The study presented comprehensive overview of existing IDS applications on soft computing, with extensive review of current IDS in soft computing, in

addition, this study used analytical approach to investigate and assess the effectiveness of considered IDS in soft computing. The result of our study shed light to researchers for future work.

1.1. Intrusion Detection System

IDS is described as anything that compromises the triangle of CIA. According to Chandrashekar and Raghveer [13], IDS is a detection mechanism that monitors network and system activities for any potential unauthorized or malicious attempts, threats or policy violations.

Typically, an IDS consists of three major functional components which are viz: an information source that provides a record of event, an analysis engine that checks and finds signs of any intrusion and a decision-making system that applies some rules and policy as a basis of the analysis engine and decides what measures should be taken based on the analysis engine outcomes. Based on the functionality, mainly the intrusion detection can be classified into anomaly detection and misuse detection. Anomaly detection IDS is based on checking the profiles of normal behaviours of the network traffic to detect whether the system carry out any unusual behaviour or not. As for misuse technique IDS, attack signatures are diagnosed by comparing the actions that correlate to any attack signatures and signal intrusion when there is a match.

1.1.1. Attack pattern

Mukkamala et al [14], noted that there are four categories of attack pattern in IDS. These core attack patterns are detected and collected as raw datasets input to networking environment log. These categories of attack are discussed below.

- **Denial of Services (DoS):** DoS is an attack pattern which occurs when an attacker aims to shut down the system out by engaging its computing facilities or memory resources. Here the attacker sends multiple legitimate requests, intended to overwhelm the system, thus denying legitimate user access to the network.

- **Probing:** Probing is an attack which occurs when an attacker scans a network to gather information or to find known vulnerabilities. On getting to know the weaknesses (or vulnerabilities), the hacker can now launch the attack based on the weaknesses.

- **User to Root (U2R):** User to root exploits is an attack where an attacker begins access as a normal user account on the system. By doing this, it enables the attacker to exploit certain potential vulnerability after gaining the root access. An example of this exploit is buffer overflows.

- **Remote to User (R2U):** Remote to User is an attack pattern where an attacker sends packets to a machine over a network and exploits the machine vulnerability by accessing it illegally and act as local user. Most of this attack is done through social engineering technique.

1.2. Soft-computing

Soft computing differs from hard computing [15], because It is literally an innovative approach that owns an emergence characteristic in order to computationally construct an intelligent system which imitates the extra ordinary of a human mind in terms of reasoning and learning[].

According to Abraham et al [17], the guiding principles of soft-computing are to exploit the tolerance for imprecision, uncertainty, low solution cost, robustness and partial truth to achieve tractability and better relationship with reality. Specifically, soft computing comprises of several computational intelligence components. They are Artificial Neural Network (ANN),

Fuzzy logic, Evolutionary Computation [18], probabilistic computing and it has similarities with Artificial Immune System (AIS), which are all related and sometimes complements each other.

Based on soft-computing systems, integrated systems known as hybrid systems are used. In hybrid systems, the approach combines two different algorithms that interact in an inseparable manner. A hybrid system is a combination strategy that can be paired together back and forth in various times with different approaches in order to achieve the best solution for the targeted issue [15]. In other words, soft-computing can be considered as a dedicated field in problem solving methods capable of simultaneously exploiting numerical data and human knowledge using mathematical modeling and symbolic reasoning systems. Soft-computing differs from traditional (or hard computing) in the aspect of not been intolerant of imprecision, partial truth and uncertainty.

Quantitative and qualitative information are used in the course of the exploration of soft-computing methodologies. These methodologies are categorically classified as soft as the human brain. The emulation of the human brain upon which all sophisticated machines is developed is the inspiration upon which they (soft-computing algorithms) are been developed.

1.3. Soft-computing in Intrusion Detection System (IDS)

In accordance to the way an IDS works, the intrusion detection can also be associated with soft computing to achieve better performance and deal with harmful intrusion. Based on previous research works [17, 19,20], there are various on-going attempts to associate data mining and machine learning techniques in addressing the problems of anomaly and misuse in intrusion detection. Following the emergence of intelligent learning mechanism, the machine learning techniques are associated with soft-computing. These techniques are developed in order to design and achieve a more intelligent intrusion detection model. Coherently, different approach, ranging from single, hybrid and cross approach has been employed in literature for a better performance measure with high accuracy detection and low false alarm rate in IDS.

1.4. Sections Organization

The current authors reviewed recent documented works concerning soft-computing and intrusion detection system. The review cut across the different principal components of soft-computing. The next section discusses single algorithm approach, the hybrid application is surveyed in section 3, Section 4 outlines the new proposed cross method, section 5 gives the contributions and limitations of soft-computing techniques and section 6 concludes the paper. Meanwhile, section 2, 3 and 4 include subsections which highlights discusses Issues in each approach of soft-computing methods.

2. Single Algorithm Approaches in Intrusion Detection System (IDS)

IDS have been implemented using various techniques in soft-computing. This section explores the application of heuristics and meta-heuristics algorithm in IDS. Intrusion detection system has been considered using a single soft-computing algorithmic approach; we attempt to review some of the algorithm as thus:

2.1. Artificial Immune System in Intrusion Detection System (IDS)

Artificial immune system attempts to imitate the human immune system (HIS). HIS is characterised by the detection and prevention of suspicious activity, be it coming from internal or external systems.

A number of model are used in AIS algorithm, literature [21,22] discussed the uses of self and non-self models. This model is based on the system to distinguish its elements and external member. Khannous et al [22] stressed the usage of the model for security of mobile ad hoc network (MANET). [9] discussed a number of literatures on AIS approaches in detecting intrusions. Artificial immune system has a tremendous edge over other algorithm in its ability to protect the system against harmful or unwanted activities upon detection [21].

[22] explored the danger theory to see into setbacks in the use of self and non-self model. The security system of proposed scheme is prone to attacks as a result of its functions. Unlike the conventional connection [22], wireless is generally known for its security vulnerabilities. Besides, they also claimed for a certainty in the detection of internal and external systems. The danger theory introduction, immune memory models, colonial selection, and negative selection algorithm for detection analysis. This proposal follows the danger theory with use of B and T cells concept. It addresses the challenges of the widely used model which is it's scalability in real world scenario.

Another research by [23], used the artificial immune system method for the protection of Mobile network security threat. The work also includes the authentication of migration from source to destination. This approach is triggered at the point of the Mobile agent migration [10]. Meanwhile, there are on-going research on HIS in order to better understand and implement it. This would enable the AIS to take gradual and full advantage of its potential.

2.2. Differential Evolution in IDS

In literature a novel based clustering algorithm had been proposed to address the wireless sensor network security challenges. Energy run-out and death eventualities attributed to the sensor challenges. An analysis of the implementation can be found in [24].

Another work by [25] implemented the IDS using the differential evolution, for the feature selection. IDS entails the detection of harm following the huge number of irrelevant and redundant data. The feature selection algorithm of DE addresses the issue. The algorithm is compared with genetic algorithm and particle swarm optimization using the KDD Cup 1999 dataset. Result shows that DE for the detection system is more efficient in the correctness of the classification. In addition to the two techniques viz: misuse and anomaly, specification based technique is also discussed in literature (e.g. [26]). Misuse detection IDS is based on predefined attacks, this gives rise to the fact that it cannot detect new attacks. Anomaly studies the normal scenario of the network and launches attack upon strange scenario detection. While specification-based techniques entail a set of specified patterns upon which detection would be based. Specification is time consuming due to the scalability of the specification [26].

2.3. Fuzzy Logic in Intrusion Detection System (IDS)

Literature has proposed different approach to fuzzy based IDS, among which are: fuzzy logic controller [27], fuzzy sets based agent communication for tactical MANET, biologically inspired type-2 fuzzy set [28,29] and etc. Ad hoc on demand distance vector was implemented using fuzzy logic in intrusion detection to address routing attacks [30]. The approach discovers malicious nodes at each node locally since IDS is on each node. The result shows that IDS detects the black hole and gray 5 hole, based on monitored traffic. However, [30] claimed that the simulation gave an accurate result when fuzzy logic is employed than when it is not used.

3. Hybrid Algorithm Approaches in Intrusion Detection System (IDS)

Generally, hybrid approach is a combination of different algorithms. The idea of this hybrid approach is to improve the accuracy of the intrusion detection system compared to implementing with single approach. The term hybrid and integrate are interchangeably used in describing a combination of two or more different approaches.

Typically, a hybrid approach consists of two functional components. The first one is aimed at handling the raw data as input and generates intermediate results. The second one will then handle the intermediate results as the input and produce the final results [31]. The raw data can be preprocessed with various classifiers and clustering based algorithm. The results are later optimized by applying the second algorithm as an integration model.

Through the years, many researchers have proposed different types of hybrid approach that combines the best and suitable hybrid approach which results in a better accuracy in IDS. In this section, some latest trends in soft computing base on hybrid implementation of intrusion

detection system are discussed.

3.1. Independent Component Analysis (ICA) with Support Vector Machine (SVM)

A hybrid approach of ICA with SVM based IDS has been proposed by [18]. This hybrid approach combines different scheme of data mining techniques; they are unsupervised and supervised learning. ICA is a computation for separating a multivariate signal into additive subcomponents. ICA has a relevant feature which acts as a removal of any irrelevant features that could deteriorates the performance or accuracy of the classifier. The motivation of a feature selector can be described as:

- The selected features simplified the classifier
- Improved the accuracy of the classifier and reduced the dimensionality of the data so that the classifier is able to deal with large values of data

This technique provides statistical signal processing tools for optimal linear transformations in multivariate data and is well-suited for feature extraction, noise reduction, density estimation and regression. SVM has been proposed as a novel technique for intrusion detection. It is also known to be a powerful tool in solving classification problems. SVM is able to classify different groups of data into either normal or anomalous distribution pattern. SVM can be classified into three:

- Divides data into normal and attack data using the binary classifier characteristics
- Implements an anomaly detection model using one-class SVM
- Combines and establishes multi-class SVM where the binary classifier divides the data into normal data and different types of attack data

In this hybrid approach, the ICA acts as feature selection which selects the best attribute of the datasets used in experiment conducted before applying SVM in classifying the data into different groups of normal and anomaly distributions. As a result, the proposed approaches are able to improve the performance of anomaly intrusion detection and reduce the false alarm rate.

3.2. Kernel Principal Component Analysis (KPCA) with Genetic Algorithm (GA) and Support Vector Machine (SVM)

Another hybrid approach based IDS has been proposed by [32] which combines SVM with KPCA and GA. The main reason that these approaches were integrated is due to the traditional problem in the IDS which results in low detection capability against the unknown network attack, high false alarm rate and insufficient intelligent analysis learning capability. In solving the problem occurrences, machine learning algorithm is adopted where it automatically improves the performance with the incremental experience.

In this method, SVM is adopted to act as a classifier to know whether an action is an attack or not. As also mentioned by [18], SVM is a novel technique that is used as a classifier in IDS. Although SVM is claimed to be the most efficient ones to be adopted as classifier, this algorithm does have limitations; in dealing with large value of datasets, the algorithm will produce large numbers of support vectors which in turn increases the training time. This is where KPCA comes into picture to enhance the detection precision for low frequent attacks and detection ability and it is also a common method used in reducing dimensional data and shortening of training time. As for GA, it is employed as an optimization factor where it is required to solve and approximate the optimization and search problems. The results of these integrated approaches are able to produce a higher predictive accuracy, faster convergence speed and produce better generalization.

3.3. Principal Component Analysis (PCA) with Genetic Algorithm (GA) and Support Vector Machine (SVM)

Another research by [33], proposed an optimized hybrid approach of IDS using soft computing techniques which are PCA, GA and SVM. The combination of these algorithms resulted in providing an optimal intrusion detection mechanism which is capable of minimizing the amount of features and maximizing the detection rates.

PCA transforms the input samples of the datasets into a new space while GA is used for optimization and SVM is for the classification purposes. PCA works as feature reduction which will speed up the training and testing process for the attack identification system but despite this, it will reduce the training efficiency and accuracy. As a countermeasure, GA and SVM is employed which provided optimization for detection models of features and parameters. This eventually minimizes the number of features and maximizes the detection rates. Without the implementation of PCA, the use of GA and SVM will only produce inconsistent and unorganized data. With PCA, the dimensionality of the dataset will be reduced but still retain the originality of the data variables [34].

3.4. Fuzzy C-Means (FCM) Clustering with Neural Network (NN) and Support Vector Machine (SVM)

A fusion of three algorithms were applied [13] which are Fuzzy C-Means (FCM) clustering, Neural Network (NN) and Support Vector Machine (SVM). FCM is a clustering algorithm that separates data into several clusters. In data clustering and classifying, the method is simpler, less time consuming and better compared to hierarchical clustering.

NN is adopted to achieve balance between the ability to respond correctly to the input patterns and provide reasonable responses to similar inputs during the training phases. This results in a reduced number of data attributes. Finally, the SVM is applied as a classification system in order to detect intrusion. This proposed fusion approaches is claimed to be valid and better in achieving detection accuracy on several attacks types such as 99.96% for DoS attacks, 99.73% for probe attack, 99.83% for R2U attack and 99.8% for U2R attack compared with other existing techniques [13].

3.5. Hierarchical Clustering Algorithm and Support Vector Machine (SVM)

Horng et al [35] proposed a novel intrusion detection system based on hierarchical clustering and Support Vector Machine (SVM). This hierarchical approach, though, was previously mentioned in [1], has lower performance than the clustering and classifying algorithm which claims to act as the key performance in providing a high quality, abstracted, and reduced dataset for SVM training purposes. Abstracted means the hierarchical clustering provides a set of equally range high data points as training sets for high detection rate and low false alarm rate. This is due to the limitations of SVM where it is unable to operate at such large datasets due to memory insufficiency which caused system failures. The overall result of this approach lead to reduction of training time and improved performance result of SVM. Besides, it also improves the accuracy of intrusion detection.

3.6. Multi-layer Perceptron (MLP) and Radial Basis Function (RBF)

A hybrid of two classification methods had been proposed in literature (for example [20]), Multi-layer Perceptron (MLP) with Radial Basis Function (RBF). Classification accuracy is determined by the ability of the system to identify normal attacks as normal and abnormal attacks as abnormal. Both of these approaches are categorized as supervised learning scheme.

The MLP is an artificial neural network model that maps sets of input data unto a set of appropriated outputs. It consists of multiple layers of nodes in a directed graph. The output is calculated by finding weights while RBF is also a network that is simply being train almost the same way as MLP. Though, MLP is a feed forward NN which also adopts back-propagation (BP) learning style in some cases while RBF adopts a feed forward (FF) learning style.

Based on Govindarajan et al, during the training phase, the MLP and RBF classifiers is used to construct a model which provides a maximum generalization accuracy of the unknown data. The test data are then passed through the saved trained model to detect intrusions in the testing phase. The overall performance of this hybrid approach was compared with the single approach and it provides an insignificant improvement of prediction accuracy in intrusion detection system.

4. Chaos Theory and Cuckoo Search Algorithm for Intrusion Detection System (IDS)

Previous section briefly described some approaches of soft-computing in Intrusion Detection System to ensure the network system is free from any unknown operations. However, there are some soft-computing approaches which have not been explored in Intrusion Detection Systems such as Chaos Theory and Cuckoo Search Algorithm.

4.1. Chaos Theory

Chaos theory is one of the soft-computing approaches in identifying sufficient solutions for unpredictable random behaviour. To simplify the definition, [36] give a statement to depict the "Chaos Theory" as the possibility of tiny causes that could bring great consequences from the initial conditions.

4.1.1. Chaos Theory: History

The term "Chaos Theory" is not new and it existed for hundreds of years after a group of astronomers discovered the planet's motion in space based on a series of phenomenon prediction. However, it was not really in use as at that time due to several arguments for uncertainty of the outcome. In 1963, the term "Chaos Theory" was officially used by Edward Lorenz, a mathematician from Massachusetts Institute of Technology (MIT) while he is trying to do a calculation for weather prediction with uncontrolled constraints. The continuous study in weather prediction was extended to a higher degree. In 1972, Lorez came out with an idea of "Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?". This idea does not cross our minds to use mathematical approaches in calculating the relationship of unpredictability for non-scientific events [36].

Planet's motion in space might be a heavy sample in illustrating the chaos theory. One of the simplest examples involving chaos theory is the effect of moving on the decimal point. Change in a single decimal point will produce a big difference if we do some operations on it. For instance, the end value of 0.525% after some mathematical operation is not identical with 0.53% (approximating into 2 decimal places).

4.1.2. Chaos Theory: The success in other fields

Research study on how chaos theory is being applied in industry is minimal compared with other soft-computing approaches. Chaos theory provides the hypothesis on how the incomplete events will produce great consequences in future through reasoning process. [37] conducted research on chaos theory and believed that till date there is no conceptual framework developed to integrate the chaos theory into industry exercise.

Several works that make use of the benefits of chaos theory such as cryptography, robotic, population models, hydrology, cardiotography, medicine, polymer, trading system, traffic system, psychology, management and sciences has been proposed. Most of them employed chaos theory with other conventional approaches to form a hybrid structure and it assures high accuracy [38]. [39] Suggest a combination of chaos theory with fuzzy logic and other combinations of chaos theory with neural network to be a good problem-solving approach. Prediction outcome makes it possible to learn through the history from previous state and psychological behaviour.

4.1.3. Chaos Theory in Intrusion Detection System (IDS): What is the barrier?

IDS need paramount efforts in detecting anomaly intrusion pattern. Most of the IDS work

concern on detection and optimization. However, not much applied the prediction theory to reduce the network/system damages that comes from intrusion. Up till now, works involving chaos theory as rules to govern IDS issues remain few.

In literature (for example [40]), chaos theory and Artificial Neural Network (ANN) were used as mechanism to detect and differentiate the traffic flow in Distributed Denial of Service (DDOS) and legitimate burst traffic. The utilization of principle "predictable" and "Characteristic Lyapunov Time" make up the result as 95% accuracy obtained from the data sample. [41] implement the chaos theory in predicting the new intrusion for small scale network range. However, the proposed works need to extend the workability in IDS real-time based. Oestreicher et al [42] in his work listed out 15 principles of chaos theory based on historical steps. Table 1 summarized few principles of chaos theory in line with IDS.

Table 1. The matching principle of chaos theory in IDS
(Indicator: Y = Yes, to apply and N = No, not to apply)

Chaos Theory principle	Description	Compatible with IDS? (Y/N)	Reason to apply/not to apply
Causality principle	Small cause able to produce great effect	Y	The fact of system is defect free from the threat due to its imperfection.
Determinism	The effect physically determined by unbroken chain of cause	Y	Based on classical model for anomaly detection, the infected system may experience the same impact with known intrusion such as high in system usage, heavy traffic flow and resource starvation
Predictability	The ability to assume the state of being certain	Y	Reverse-engineering by studying after attacks was done to analyse before the attack was start which can learn from the common impact lessons. [18]
Models	Architecture designed to show how the systems being correctly working	Y	IDS models consist of several components (detection and prevention) in order to reduce system's damage.
Dynamical system	System changes over the time cause by causality principle and determinism	N	IDS stay on the current state and only the database keep updating for new intrusion pattern
Phase space	Each possible state communicate to unique point in the phase space	Y	Most of the intrusions detected in IDS correlates
Sensitive to initial conditions	Change in one variable factorises to different consequences	Y	In many systems, vulnerabilities keep growing as one variable changes and require a mechanism like IDS to stop it
Integrable system	The ability of the system to engage with another system	Y	IDS may integrate to another system such as Access Control System to boost up the performance by observing the intrusions in different dimensionality
Linear system	No hidden layer between input and output	N	There are various conditions that are potentially exploitable and considered as non-linear system
Attractor	Dynamic systems evolves after a long time	N	IDS keep evolving as new intrusion comes in which tracking them randomly
Characteristic Lyapunov time	A timescale on which a dynamic system is in chaos situation	Y	Attacker could evade the IDS filtering by overloading the security channel causing a flooding packet in IDS traffic [19]
Feedback	Response from the system either as positive feedback or negative feedback	Y	IDS monitor and detect abnormal network traffic and generates alarm as a feedback to security admin for intrusion presence
Self-similarity	Each objects that composed from subunits corresponds as one entity	Y	Particular system/network composed by multiple components with strong relationship in order to produce firm entity
Fractal	Geometrical object fulfil two characteristics: self-similarity and fractional dimensionality	Y	Suitable for known intrusion pattern
Fractal dimension	The fractal pattern reflecting the scale	Y	Suitable for known intrusion pattern

From a general point of view of IDS, the chaos theory is compatible with minor similarities with IDS nature. IDS possess characters of inherently unpredictability for small fraction of IDS system [43] and

a part of it, some vulnerabilities are not able to be defined at the early stage. For this reason, attacks will come from every corner of technology; there exist less potential in identifying a new intrusion pattern. Most of the risk exposure appear from software itself due to poor software development, uncertain complexity, much depending on outsource and lack of appropriate management [44] besides inherent problems on network equipment and network services.

4.2. Cuckoo Search Algorithm

Cuckoo Search Algorithm is a new optimization algorithm in soft-computing domain. Few experiments in some applications have promising and good result in forming a self-organizing system. The system serves global optimization problems. Optimization is achieved when there is a trade-off between essential things with low-cost (or less work solutions) to produce the same output or even greater than it current solution [45]. This subsection discusses the acceptance of Cuckoo Search Algorithm in extending its capability in Intrusion Detection System domain.

4.2.1. Cuckoo Search Algorithm: History

Cuckoo Search Algorithm was developed by Yang et al [45]. This optimization algorithm is an inspiration of nature appearances of cuckoo's certain species which breeds the population by leaving its eggs in another bird's nest. Cuckoo birds are called lazy birds but they do have strong motivation. The reason why cuckoo leaves the eggs is because they do not build any nest for themselves for shelter. Young cuckoo fully depends on other birds to keep them alive. Cuckoo's mother reduces risky exposure of the eggs by obtaining a shelter elsewhere. To lay the eggs, cuckoo will choose other host bird's nest containing eggs and lay theirs to fool the owner that the new eggs belong to them. After the young cuckoo grows up, it will throw out the rest of the eggs while the foster parents feed them like their own family member. After some time, this young cuckoo migrates to another place leaving their foster parents.

For some clever host birds, they are able to detect and manage the intruder by throwing out the unknown eggs or simply abandoning the nest to build a new one. Initially, [34] introduced Cuckoo Search Algorithm as a new optimization strategy to serve for multimodal objectives with various constraints. The advancement of Cuckoo Search Algorithm continuous research work is to enhance and provide better solutions in optimization technique.

4.2.2. Cuckoo Search Algorithm: The success in other fields

Cuckoo Search Algorithm has been applied in many domains to measure and prove the efficiency. Some of the previous works operate using a single algorithm approach and some of them operate in hybrid combination such as PSO and GA. Through the research studies, Cuckoo Search Algorithm shows a degree of productivity which is higher than PSO and GA achievements. It has proved to ensure global convergence by which it assists in multi-objective problems and it is time efficient for searching globally and local propagation as well [46].

Various applications have been applying the Cuckoo Search Algorithm. Such as in manufacturing fields (engine production and optimization approaches), computer engineering (wireless sensor network), Job Scheduling, Cryptography, Software Development and Computational Complexity Theory Engineering (Optimization approaches and Integrated Circuit) and others.

4.2.3. Cuckoo Search Algorithm in Intrusion Detection System (IDS): Is it possible?

Up till now, there are few papers discussing on how to implement Cuckoo Search Algorithm to be a part of IDS technique. [47] carried out the operation to be tested in Wireless Sensor Network domain. Based on the workflow done by authors, the combination of PSO and Cuckoo Search Algorithm present a good result in reducing energy consumption and finding the optimal path for intrusion detection employed in wireless sensor network. Our study on Cuckoo Search Algorithm found the characteristics of Cuckoo Search Algorithm as below:

- Multi-objective optimization
- Solving for non-linear problems
- Guarantee for global convergence
- Time efficient in seeking global and local solution path (Faster search rate)

By taking this advantages and match with IDS cases, it is possible to improve the IDS performance efficiently, reliable result and suitable solution to aim for low-cost and less job with high productivity and accuracy.

4.3. Discussion

In section 2 study proposed in [26] were not able to stand all kinds of attack due to the sole use of distributed architecture. A hybrid of cooperative and distributed architecture would be a better choice. The combination of two or more heuristic algorithm going hand in hand will give a better performance output.

In section 3 following the adoption of more than one algorithm to form a hybrid approach, we made some observations. The observation is that the recent hybrid approaches use SVM as the base classifier for IDS [18]. This is due to the fact that SVM is currently one of the most efficient algorithms in classifying data into normal and anomaly intrusion pattern. Despite its effectiveness as a classifier, SVM as a single approach is limited to low performance level when applied on high dimensional datasets. Also, due to the parameter selection, it increases the training time when a large support vector is produced.

While other algorithms such as PCA and KPCA [32] and [33] respectively lie under the same category as SVM, it acts as a factor analyser that enhances the detection process. KPCA is the extension of PCA algorithm if it applies the kernel method. Kernel method is a class algorithm of pattern analysis and works closest to the SVM. With pattern analysis, it does a perfect job in finding general types of relationship including cluster's number. As for FCM clustering, it is being used to group the data into several clusters before proceeding into classifying the data into different attack pattern. Several issues should be focused in applying hybrid approach-based IDS:

- Determining whether the specific algorithm could be used to address existing problems in intrusion detection area
- Hybrid algorithms approaches should deal with certain performance measure such as detection rate, false alarm rate, trade-off between detection rate and false alarm rate, overall performance and fault tolerance.

In summary, the work of each hybrid approach is varied, there is not one solution that could deal with all the issues in intrusion detection. Every hybrid approach serves different measure and occasionally different methods is specified only for certain attack pattern as there are so many variables involved that even a good method with good accuracy may not be the best solution because it may end up with too many computational resources.

In section 4 all theories mentioned [36-44] have never been employed in any IDS works. The research area for the theories needs an extensive study before developing the prototype and conducting empirical testing to prove the efficiency in predicting and assorting the new pattern of attacks. It is important to figure out few considerations. [43] addressed several key parameters in measuring the efficiency of IDS which are:

- Accuracy in eliminating false alarms
- Performance of detecting process
- Completeness to detect all attacks
- Fault tolerance in resisting to all kind of attacks
- Timeliness to alert security administrator of intruder's presence

Critical phase in most of the IDS works are in making a decision on how to eliminate false positive and false negative. It represents the theory to be intelligent enough and acceptable in classifying illegal and legal activities especially in very large scale network environment where dynamic structure applied to serve better connections. [48] believed false positive and false negative remain a big challenge for most IDS works because it can't provide 100% accuracy in detecting the intrusion correctly.

5. Summary

This section provides the limitation, conclusion and recommendation of the overall scope of the paper review.

5.1. Limitation and conclusion

This paper gave a survey on methods used in IDS. This is done by the use of single, hybrid methodologies in soft-computing. The system issues have been addressed using the aforementioned approaches [39]. [23] pointed out setbacks from literature which includes among others; high installation cost of new equipment, large production of log files and slow performance. However, for further research, the limitations are in the security of the network irrespective of the scalability, the inefficiency of the threat identification, protection and detection of the threats. However, a more understanding of the natural algorithm would facilitate the potential discoveries which would be executed on the artificial scenario. Further research would focus on the chaos theory and cuckoo's search algorithm exploration and implementation.

5.2 Recommendations

Meanwhile, the current author supports [49] in recommendation of associative security mechanism to be more effective than its singular application. Figure 1 shows the overlapping effect of confidentiality and integrity. Also, [50] a refined security threat measure to ascertain the reliability and protection of the network system is needed to be adopted for a better performance.

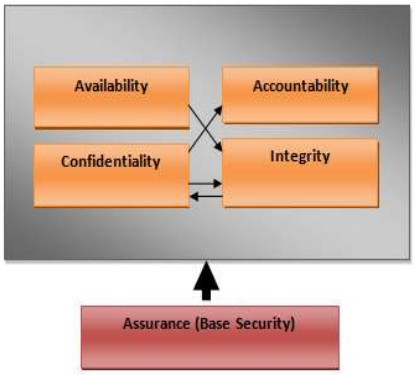

Figure 1. Overlapping effect [49]

References

[1] Shenify M. "Trusted Node-Based Algorithm to Secure Home Agent NATed IPv4 Network from IPv6 Routing Header Attacks". TELKOMNIKA (Telecommunication Computing Electronics and Control). 2014 Dec 1;12(4):969-76.

[2] Xuewu Z, Huenteler J. "Classification Recognition Algorithm Based on Strong Association Rule Optimization of Neural Network". TELKOMNIKA (Telecommunication Computing Electronics and Control). 2016 Jun 2;14(2A):241-7.

[3] Wang H, Ma R. "Design of Neural Networks for Intrusion Detection". TELKOMNIKA (Telecommunication Computing Electronics and Control). 2016 Sep 1;14(3A):321-5.

[4] Aliero MS, Ardo AA, Ghani I, Atiku M. "Classification of Sql Injection Detection And Prevention Measure". IOSR Journal of Engineering (IOSRJEN), ISSN (e). 2016:2250-3021.

[5] Aliero MS, Ghani I, Zainudden S, Khan MM, Bello M. "REVIEW ON SQL INJECTION PROTECTION METHODS AND TOOLS". Jurnal Teknologi. 2015 Nov 12;77(13).

[6] Nkiama H, Said SZ, Saidu M. "A Subset Feature Elimination Mechanism for Intrusion Detection System". International Journal of Advanced Computer Science and Applications. 2016 Apr 1;7(4).

[7] Elhag S, Fernández A, Bawakid A, Alshomrani S, Herrera F. "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems". Expert Systems with Applications. 2015 Jan 1;42(1):193-202.

[8] Abraham A, Jain R, Thomas J, Han SY. D-SCIDS: "Distributed soft computing intrusion detection system. Journal of Network and Computer Applications". 2007 Jan 1;30(1):81-98.

[9] Aliero MS, Ghani I. "A component based SQL injection vulnerability detection tool". InSoftware Engineering Conference (MySEC), 2015 9th Malaysian 2015 Dec 16 (pp. 224-229). IEEE.

[10] Sahasrabuddhe A, Naikade S, Ramaswamy A, Sadliwala B, Futane P. "Survey on Intrusion Detection System using Data Mining Techniques". International Research Journal of Engineering and Technology (IRJET), 2017 May Volume: 04 Issue: 05

[11]] Jacob NM, Wanjala MY. A Review of Intrusion Detection Systems. Global Journal of Computer Science and Technology. 2018 Jan 12.

[12] Agrawal S, Jain G. "A Review on Intrusion Detection System Based Data Mining Techniques" International Research Journal of Engineering and Technology (IRJET), 2017 Sep Volume: 04 Issue: 09

[13] A. Chandrashekar and K. Raghuveer, "Fusion of multiple data mining techniques for effective network intrusion detection: a contemporary approach," in *Proceedings of the Fifth International Conference on Security of Information and Networks*, 2012, pp. 178-182.

[14] S. Mukkamala, A. H. Sung, and A. Abraham, "Intrusion detection using an ensemble of intelligent paradigms," *Journal of Network and Computer Applications,* vol. 28, pp. 167-182, 2005.

[15] C. Langin and S. Rahimi, "Soft computing in intrusion detection: the state of the art," *Journal of Ambient Intelligence and Humanized Computing,* vol. 1, pp. 133-145, 2010.

[16] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Applied Soft Computing,* vol. 10, pp. 1-35, 2010.

[17] A. Abraham and R. Jain, "Soft computing models for network intrusion detection systems," *arXiv preprint cs/0405046,* 2004.

[18] S. Pilabutr, P. Somwang, and S. Srinoy, "Integrated soft computing for Intrusion Detection on computer network security," in *Computer Applications and Industrial Electronics (ICCAIE), 2011 IEEE International Conference on*, 2011, pp. 559-563.

[19] S. Revathi, & Malathi, A. Exploration of Hybrid Soft Computing Techniques for Intrusion Detection [Online].

[20] M. Govindarajan and R. M. Chandrasekaran, "Intrusion detection using neural based hybrid classification methods," *Computer Networks,* vol. 55, pp. 1662-1671, 2011.

[21] U. Aickelin, J. Greensmith, and J. Twycross, "Immune system approaches to intrusion detection–a review," in *Artificial Immune Systems*, ed: Springer, 2004, pp. 316-329.

[22] A. Khannous, A. Rghioui, F. Elouaai, and M. Bouhorma, "A New Approach to Artificial Immune System for Intrusion Detection of the Mobile Ad Hoc Networks," *International Journal of Computer Applications,* vol. 92, pp. 50-53, 2014.

[23] Z. Brahmi, A. Lini, and M. M. Gammoudi, "Mobile Agent Security Based on Artificial Immune System," in *International Joint Conference SOCO'14-CISIS'14-ICEUTE'14*, 2014, pp. 385-395.

[24] P. Kuila and P. K. Jana, "A novel differential evolution based clustering algorithm for wireless sensor networks," *Applied Soft Computing,* vol. 25, pp. 414-425, 2014.

[25] S. Zaman, M. El-Abed, and F. Karray, "Features selection approaches for intrusion detection systems based on evolution algorithms," in *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*, 2013, p. 10.

[26] A. Chaudhary, V. Tiwari, and A. Kumar, "Analysis of fuzzy logic based intrusion detection systems in mobile ad hoc networks," *Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM),* vol. 6, pp. 690-696, 2014.

[27] S. Sujatha, P. Vivekanandan, and A. Kannan, "Fuzzy logic controller based intrusion handling system for mobile adhoc networks," *Asian Journal of Information Technology,* vol. 7, pp. 175-182, 2008.

[28] D. Watkins, "Tactical manet attack detection based on fuzzy sets using agent communication," DTIC Document2004.

[29] A. Visconti and H. Tahayori, "A Biologically-Inspired Type-2 Fuzzy Set Based Algorithm for Detecting Misbehaving Nodes in Ad-Hoc Wireless Networks," *INTERNATIONAL JOURNAL FOR INFONOMICS,* vol. 3, pp. 373-382, 2010.

[30] M. Wahengbam and N. Marchang, "Intrusion detection in manet using fuzzy logic," in *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on*, 2012, pp. 189-192.

[31] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *Expert Systems with Applications,* vol. 36, pp. 11994-12000, 2009.

[32] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," *Applied Soft Computing,* vol. 18, pp. 178-184, 2014.
[33] A. I. Ahmad, Alghamdi, H., Hussain, A., Muhammad, "Optimized Intrusion Detection Mechanism using Soft Computing Techniques," *Telecommunication Systems,* pp. 2187-2195, 2013.
[34] M. R. Patra and A. Panigrahi, "Enhancing Performance of Intrusion Detection through Soft Computing Techniques," pp. 44-48, 2013.
[35] S.-J. Horng, M.-Y. Su, Y.-H. Chen, T.-W. Kao, R.-J. Chen, J.-L. Lai*, et al.*, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert Systems with Applications,* vol. 38, pp. 306-313, 2011.
[36] É. Ghys, "The Butterfly Effect," in *The Proceedings of the 12th International Congress on Mathematical Education*, 2015, pp. 19-39.
[37] X. Lu, D. Clements-Croome, and M. Viljanen, "Integration of chaos theory and mathematical models in building simulation," *Automation in Construction,* vol. 19, pp. 452-457, 2010.
[38] A. Layeb, "A novel quantum inspired cuckoo search for knapsack problems," *International Journal of Bio-Inspired Computation,* vol. 3, pp. 297-305, 2011.
[39] U. K. Chakraborty, S. K. Das, and T. E. Abbott, "Energy-efficient routing in hierarchical wireless sensor networks using differential-evolution-based memetic algorithm," in *Evolutionary Computation (CEC), 2012 IEEE Congress on*, 2012, pp. 1-8.
[40] J. Cheng, J. Yin, C. Wu, B. Zhang, and Y. Liu, "DDoS attack detection method based on linear prediction model," presented at the Proceedings of the 5th international conference on Emerging intelligent computing technology and applications, Ulsan, South Korea, 2009.
[41] X.-X. Wen, X.-R. Meng, Z.-Q. Ma, and Y.-C. Zhang, "The chaotic analysis and trend prediction on small-time scale network traffic," *Dianzi Xuebao(Acta Electronica Sinica),* vol. 40, pp. 1609-1616, 2012.
[42] C. Oestreicher, "A history of chaos theory," *Dialogues in clinical neuroscience,* vol. 9, p. 279, 2007.
[43] H. Debar, "An introduction to intrusion-detection systems," *Proceedings of Connect,* vol. 2000, 2000.
[44] H. A. Julia, Sean, B., Robert, J.E., Gary, M., Nancy, R.M., "Software Security Engineering: A Guide for Project Managers," ed: Addison Wesley Professional, 2008, p. 368.
[45] X.-S. Yang and S. Deb, "Cuckoo search via Lévy flights," in *Nature & Biologically Inspired Computing, 2009. NaBIC 2009. World Congress on*, 2009, pp. 210-214.
[46] X.-S. Yang, Deb, S., "Cuckoo search: recent advances and applications," *Neural Comput & Applic (2014),* vol. 24, pp. 169-174, 2013.
[47] S. Kumar, "Improving WSN Routing and Security with an Artificial Intelligence approach."
[48] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," *NIST special publication,* vol. 800, p. 94, 2007.
[49] P. Dadhich, K. Dutta, and M. Govil, "Security issues in mobile agents," *International Journal of Computer Applications,* vol. 11, pp. 0975-8887, 2010.
[50] J. Snehi, M. Snehi, and S. Goyal, "Security threats to mobile agents," in *Proceedings of the International Conference on Advances in Computing and Artificial Intelligence*, 2011, pp. 220-222.