IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 30, 2018, accepted April 30, 2018, date of publication May 14, 2018, date of current version June 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2835166

An Efficient IDS Using Hybrid Magnetic Swarm Optimization in WANETs

ALI SAFAA SADIQ[1], (Member, IEEE), BASEM ALKAZEMI[2], SEYEDALI MIRJALILI[3], NORAZIAH AHMED[4,5], SULEMAN KHAN[1], IHSAN ALI[6], AL-SAKIB KHAN PATHAN[7], (Senior Member, IEEE), AND KAYHAN ZRAR GHAFOOR[8], (Member, IEEE)

[1]School of Information Technology, Monash University, Bandar Sunway 47500, Malaysia
[2]Department of Computer Science, College of Computer & Information Systems, Umm Al-Qura University, Mecca 715, Saudi Arabia
[3]Institute for Integrated and Intelligent Systems, Griffith University, Brisbane, QLD 4111 Australia
[4]Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Kuantan 26300, Malaysia
[5]IBM Centre of Excellence, Universiti Malaysia Pahang, Kuantan 26300, Malaysia
[6]Faculty of Computer Science & Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia
[7]Department of Computer Science and Engineering, Southeast University, Dhaka 1213, Bangladesh
[8]Department of Computer Science, Faculty of Science, Cihan University-Erbil, Erbil 066, Iraq

Corresponding authors: Ali Safaa Sadiq (ali.safaa@monash.edu) and Suleman Khan (suleman.khan@monash.edu)

This work was supported by the Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Mecca, Saudi Arabia.

ABSTRACT Sophisticated Intrusion attacks against various types of networks are ever increasing today with the exploitation of modern technologies which often severely affect wireless networks. In order to improve the effectiveness of intrusion detection systems (IDSs), data analysis methods such as data mining and classification methods are often integrated with IDSs. Though, numerous studies have contributed in various ways to improve the utilization of data mining for IDS, effective solution often depends on the network setting where the IDS is deployed. In this paper, we propose an efficient IDS based on hybrid heuristic optimization algorithm which is inspired by magnetic field theory in physics that deals with attraction between particles scattered in the search space. Our developed algorithm works in extracting the most relevant features that can assist in accurately detecting the network attacks. These features are extracted by tagged index values that represent the information gain out of the training course of the classifier to be used as a base for our developed IDS. In order to improve the accuracy of artificial neural network (ANN) classifier, we have integrated our proposed hybrid magnetic optimization algorithm-particle swarm optimization (MOA-PSO) technique. Experimental results show that using our proposed IDS based on hybrid MOA-PSO technique provides more accuracy level compared to the use of ANN based on MOA, PSO and genetic algorithm. Updated KDD CUP data set is formed and used during the training and testing phases, where this data set consists of mixed data traffics between attacks and normal activities. Our results show significant gain in terms of efficiency compared to other alternative mechanisms.

INDEX TERMS Intrusion detection, feature extraction, optimization, security, network flow analysis, computational intelligence.

I. INTRODUCTION

The tremendous advances and vogue of anywhere anytime Internet as a basic medium of online communication have made the security of Wireless Ad-hoc Networks (WANETs) one of the main issues in the current research arena. The last decade has witnessed more attention towards protecting the sensitive data from intruders and ensuring that the data transmission is performed in a safe way. Thus, Intrusion Detection System (IDS) for WANET was given relatively lesser efforts though some good works came out during that period [1]–[4]. In reality, it is not an easy task to distinguish between the attack and the normal network access especially in WANET communications [3], [5], [6]. To overcome this challenge, many Artificial Intelligence (AI) based techniques are proposed to be integrated with IDS as a way to improve its performance. For instance ANN, Fuzzy logic, SVM (Support Vector Machines), GA (Genetic Algorithm), PSO (Particle Swarm Optimization), and Hybrid systems have been studied to improve the classification rate of IDS [1], [7], [8].

In general, IDS can be categorized based on activity level into two main classes which are: Network based IDS (NIDS) and Host based IDS (HIDS) [3]. Network based IDSs are developed to monitor activities of multiple hosts and analyze WANET packets captured from the network segment. Host based IDSs are designed to monitor activities of specific host system. On the other hand, IDS has two types of strategic detection methods namely, signature recognition and anomaly detection. The difference between these methods is that signature recognition identifies intrusions depending on features of known attacks while anomaly detection analyzes the properties of normal behavior [9], [10]. Therefore, IDS deals with incredible volume of data which contain redundant and unrelated features that could introduce an extreme training and calculation time [11], [12].

Various approaches for feature reduction/classification have been proposed in order to improve the efficiency of IDS in detecting attacks [13]. Many of those are based on machine learning techniques for the purpose of optimizing IDS's feature selection, mainly for better attack classification process. Unfortunately, none of the proposed mechanisms is perfect – there are always some shortcomings. Hence, we argue that there is a need for continuous study to improve the performance of IDSs. In fact, sometimes the classification method that might be suitable for a specific problem is not easy to address. This issue is presented in a well-known No Free Lunch (NFL) theorem which states that there is no heuristic algorithm best suited for solving all optimization problems [14]–[18]. Therefore, after our thorough study, Magnetic Optimization Algorithm (MOA) has been integrated and hybridized with PSO to optimize the performance of ANN in classifying network traffic of IDS. The main contribution of this work is to achieve a robust classifier that could assist in constructing an accurate IDS, which secures the WANETs. In other words, our proposed MOA-PSO algorithm has improved the detection and classification rates to increase the efficiency of IDS.

This paper mainly focuses on detection as well as classification of network traffic that labeled as Normal, Smurf Attack, and Neptune Attack using our optimized ANN. Also, we would like to highlight that one of the main limitations that this work faced is the highly dynamic sample of network attack (due to some applied network policies).

The remainder of this paper is structured as follows. In Section II, we present the related work. Section III discusses the main concept of MOA technique as well as the methodology of our proposed IDS based on hybrid MOA-PSO. The simulation results and performance analysis are illustrated in Section IV, and finally, Section V concludes the paper with the future research directions.

II. RELATED WORK

Various optimization techniques are proposed by researchers to achieve high accuracy in IDS. In this section, some of the previous works and methods are discussed including hierarchical clustering algorithm [5], [19] removal feature selection and SVM [18], gravitational search algorithm [20] and pattern recognition [19]. We would talk about a wide range of related works that have motivated us in devising our approach.

The combination of hierarchical clustering and SVM is proposed in [5], where the authors use Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH) algorithm to alter the KDD CUP 1999 dataset [21] to reduce the dataset. Besides, the algorithm is used to produce a reduced high quality dataset from the original KDD CUP 1999 dataset before training the SVM. BIRCH is an unsupervised data mining algorithm used to perform hierarchical gathering over principally huge datasets. The experimental result using the proposed technique achieved high accuracy, which is 95.72%. Also, it is shown that the mechanism produces low false positive rate, around 0.7%. However, the number of instances tested in this work was quite less than the original KDD Cup 1999 dataset. Besides, BIRCH algorithm can only handle numeric data and it is sensitive to the order of the data record. In addition to that, BIRCH algorithm prefers only clusters with spherical shape and similar sizes of data to perform high performance of classification.

On the other hand, Gradually Feature Removal (GFR) algorithm is proposed in [7]. The authors have used 19 (nineteen) important features to build the IDS's judgment of WANET visitors to be categorized as normal or not. Clustering method is proposed using ant colony algorithm and SVM. The authors also have used combination feature selection method, which combines wrapper and filter methods to achieve better performance. The first step is Data preprocessing where it constructs the raw database and deletes the repeated data. Afterwards, they train the dataset using ANN which classifies the data into 41 features of KDD CUP '99 as a way to discover the best training samples that can achieve high accuracy. Last step is the feature reduction to train the dataset and test the model with 41 features and 4 different features of reduction techniques until they have achieved 19 important features that were chosen by GFR algorithm. The accuracy achieved by applying this method was 98.62%, which indicates that it performs well with high accuracy and efficiency. However, as we have investigated, the ant colony algorithm along with the proposed GFR incurs high computational cost especially with huge datasets. Thus, we can assume that the proposed method in [7] could obtain less accuracy with more complex dataset due to the aforementioned reasons.

As an effort to improve the performance of IDS, Gravitational Search Algorithm (GSA) is proposed in [20] to support Artificial Neural Network in IDS. The GSA is a popular algorithm that utilizes machine learning based on gravity law and interaction of mass. The concept of magnetic force was firstly proposed for training ANN/MLP (Artificial Neural Network/Multi Layer Perceptron) in our previous work in [11]. Dastanpour *et al.* [20] have divided the KDD CUP '99 dataset into two phases: one is used for testing while the other for training. The experimental results show that the

ANN supported with GSA produces high accuracy (98.7%) of detection rate, meaning that GSA method could optimize and improve the ANN performance in classification. Besides, the method also could achieve 100% accuracy with only 39 critical features of KDD CUP '99. However, the proposed method could perform better by hybridizing it with other evolutionary optimization algorithm as a way to cope with various and more complex types of datasets.

Tian and Liu propose in [15] a new IDS model using hybrid ANN and PSO algorithms. By introducing PSO, they could minimize the limitation of searching efficiency within complex IDS's dataset. They utilize the rough set as data of ANN to select a subset of input attributes and employ the PSO algorithm to optimize ANN performance. Eight of rough set features have been selected and the ANN output layer consisted of six nodes. Five of the output nodes were used to represent four types of IDS attacks and one for normal behavior. The training and testing sets were set as 80% and 20% respectively, where the total number of the data was 460. The proposed method in [15] produced higher stability and could achieve improved attack detection rate with lower mean squared error. Though, the PSO has its own drawbacks [16], which are, getting trapped in local minima and the slow convergence rate that needs further investigation to improve its performance.

As another attempt to protect one of the most popular clustered routing protocols in Wireless Sensor Network (WSN), which is called Cluster based Low-Energy Adaptive Clustering Hierarchy (LEACH), the performance of WSN under attack scenario is thoroughly investigated in [17]. The Black hole and Gray hole types of attacks [22] are used to study the performance of LEACH and its resistance against them. A concept known as "*High energy threshold*" was utilized to simulate these attacks using ns-2 simulator. Tripathi *et al.* [17] have applied this concept to different network parameters with different node densities. They have compared the impact of both types of attacks and found that the Black hole attack is more effective on the WSN performance as compared to the Gray hole attack. The limitation of this study is that the authors conducted their work with an assumption that the malicious node in most of the time is obtaining higher energy as compared to the normal nodes to be able to run for maximum lifetime during network operation while for most of the time, malicious node launches the attack (kind of continuously) and causes the compromised node to drain its energy [23], [24]. Furthermore, considering accurate malicious detection model could essentially improve the performance of such routing protocol in saving node's energy. This will be achieved via early detection of launched attack to be blocked for the seek of preventing further wasting with network resources.

Qassim *et al.* [18] investigate the Anomaly-based Network Intrusion Detection Systems (A-NIDS). In this work, the authors highlight the limitation of existing A-NIDS as they produce an extraordinary bulk of alarms that can be varied with false-positive alarms. Such huge volumes of false alarms avoid precise recognition of network attacks that would affect negatively the instant reaction of IDS. Hence, as a way to overcome this issue, the authors have introduced a strategy for filtering such false-positive alarms of A-NIDS. They have propose a new classification technique called semi-supervised alarm which does not necessitate predefined knowledge of attack signatures or security personnel feedback [25]. However, the proposed classification technique needs further optimization in order to maintain high accuracy with dynamic changes of parameters that indicates the anomalous activities, which would vary from one network to another.

The open challenge that could be highlighted here is that the detection rate decreases significantly when the numbers of features and training samples increase [26]. Since feature extraction is a procedure of selecting a set of F features from a dataset of N features, $F<N$, the cost of some evaluation function or measure will be optimized over the space of all possible feature subsets of intrusion cases. There are still many obstacles for the feature extraction procedure to improve its accuracy in removing the non-dominant features and accordingly, its ability in reducing the training time and mitigating the complexity of the developed classification models.

It is worth mentioning that as reported in numerous studies, attempting feature extraction technique most the time contributes to enhancements in the predictive accuracy and improvements in the sensitivity, clarity, and generality of the developed model [27]. On the other hand, extracting the best subset of features that helps accurately identify the attack from all possible $2N$ subsets is not an easy task and tends to be non-polynomial complex problem during the increase of searching space [27]. By shedding the light on ANN (as the wide utilized classifier), its performance could be extremely enhanced by obtaining a systematic feature election model, as the same applies on data mining and machine learning techniques. Each method discussed above has its benefits and disadvantages; thus, a model should be developed in a way to overcome the limitation of existing methods in accurately identifying the network attacks.

Having studied all these existing IDSs, we are motivated in this paper to propose an efficient IDS based on hybrid MOA-PSO algorithm in order to overcome some of the critical limitations of the existing techniques.

III. PROPOSED METHODOLOGY AND DESIGN

In this section, our proposed methodology and design are described. A quick overview of the main concept of MOA algorithm is presented followed by its use in the field of optimization. Table 1 mentions the mathematical symbols that are used in this section. The following subsections are discussing the detailed design of our proposed method.

A. HYBRID MOA AND PSO FOR IDS SYSTEM

Recently, Multi-Layer Perceptron (MLP) has gained popularity as a computational tool and has been applied in

TABLE 1. Mathematical symbols and definitions.

Symbol	Definition
C	Cost value of seed parameters of ANN
β	Classification cycle
$x_{i,j}^{k}(t)$	k-th dimension of i,j-th agent
$B_{u,v}(t)$	Magnetic field of agent u,v
u_k	Upper bound of searching space
l_k	Lower bound of searching space
D	Distance between Masses
N_{ij}	Set of the neighboring agents
$M_{i,j}(t)$	Mass agent notation
$v_{i,j}^{k}$	Velocity of mass agent
o_i^k	Actual value of a class
d_i^k	Desired output of a class
S_P	Population size
C_{n_i}	Number of combinations
p_i	Probability form of arbitrary data sample selection

various research areas [11], [28]. On the other hand, MOA (Magnetic Optimization Algorithm) is a heuristic optimization algorithm that was proposed in our previous work [11], which is utilized in this work to overcome the limitation of MLP for achieving better intrusion classification in IDS. This algorithm was basically inspired by magnetic field theory in physics that deals with attraction between particles scattered in the search space. Each magnetic particle has a measure of mass and magnetic field due to its fitness. The acceptable magnetic particles are those with the higher magnetic field and higher mass.

As discussed in the previous section, an IDS mainly relies on the deep analysis of network traffic as a way to detect malicious activities. The detection accuracy of IDS is often dominated by the analyzed sample of the network traffic traces as well as the selected set of features [29]. Our proposed hybrid MOA-PSO runs as an analyzer sub-system that helps find the small set of features, which would assist in making decision to be used for classification. Figure 1 illustrates the general architecture of data analysis using our proposed IDS based on hybrid MOA-PSO, which consists of three main entities: default gateway, network flow collector (server), and analyzer (run based on our proposed algorithm). The analyzer detects any anomalous traffic and reports it to the network admin to update the database accordingly. Afterwards, the correlated set of features that infers the detected attack would be identified during the training phase of our algorithm.

In order to represent the individuals/population of each particular entry of IDS inspected data, we have defined decision variables to represent individuals, which are ANN parameters and inserted detection features. This process is performed during each iteration of analysis. In other words, our algorithm inspects one feature in every iteration and provides an index value to rank that feature for further extraction process.

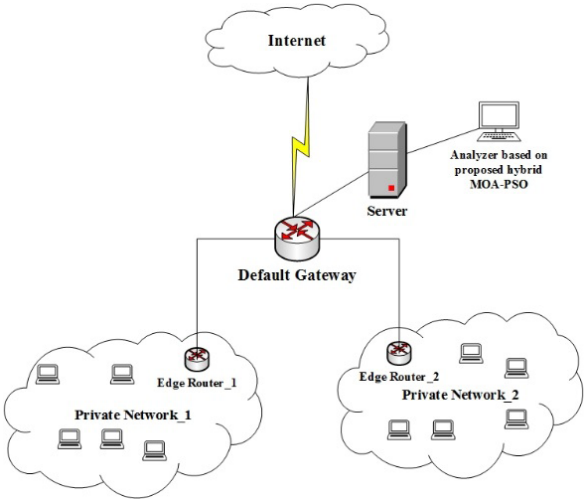

FIGURE 1. Analyzing architecture of network data flow using the proposed IDS based on hybrid MOA-PSO.

The equation, as mentioned following this text presents the cost value C of seed parameters of ANN used in each classification cycle β as well as the number of inserted features (which is in our case 41 features). A filter based method is used during feature selection process to score feature subsets. In each iteration, a score will be given to a feature subset. We used a random number generator from 0 to 1 and different combinations over the course of iterations. This type of measurement is preferred to be fast in computation, while still filtering the worth of the feature's sub-set based upon its reflected impact on the calculated output during training phase. During inspection of each feature, the feature i will be checked against the index value of f_i as a tagged value ≥ 0.5, then the score of that feature will be rounded to 1 and selected for further use in building the detection model for indicating attack i; otherwise, it will be rounded to 0 and it will be excluded from the list of sub-set features: $f_i = [C\beta F1\ F2 \ldots F_n]$. We assumed that each search magnetic swarm agent calculates its fitness value upon selecting a sub-set of features f_i and gets compared against the index threshold value during training and testing processes of the detection model. By applying this process during all iterations, eventually less competent features would be extracted as they have produced less impact on the obtained fitness value while the dominantly high indexed features would be kept in the last extracted list to be used in the finalized model.

The formula in equation (1) is used during the definition of all the epochs where the electromagnetic force is from u, v-th agent on the i, j-th agent at a specific iteration number t. i, j are used to identify the two dimension indexing cellular topology of MOA.

$$f_{(i,j),(u,v)}^{k}(t) = \frac{B_{u,v}(t)}{D\left(x_{i,j}^{k}(t), x_{u,v}^{k}(t)\right)}(x_{i,j}^{k}(t)) \tag{1}$$

Here, $x_{i,j}^{k}(t)$ is the k-th dimension of i, j-th agent at the iteration number$t$. $B_{u,v}(t)$ is the magnetic field of agent u, v at

the same iteration number t, $x_{i,j}^{k}(t)$ and $x_{u,v}^{k}(t)$ are k-th dimensions of i,j-th and u,v-th agents at iteration t. Besides, D is the function for calculating the distance between agents in the equation (2). u_k is for upper bounds and l_k is for lower bounds of the search space where m represents the dimension of the search space [11].

$$D\left(x_{i,j}^{k}(t), x_{u,v}^{k}(t)\right) = \frac{1}{m}\sum m_{k=1}\frac{x_{i,j}^{k}(t) - x_{u,v}^{k}(t)}{u_k - l_k} \quad (2)$$

Equation (3) is used to calculate the magnetic field of i,j-th agent at the iteration t. $Fitness(t)$ can be any fitness function.

$$B_{i,j} = Fitness_{i,j}(t) \quad (3)$$

In MOA, the problem in a space with dimension k, the subsequent force that acts on i,j-th agent is calculated in equation (4). N_{ij} is the set of neighbours of i,j-th agent at the iteration t.

$$F_{i,j}^{k}(t) = \sum\nolimits_{u,vinN_{ij}} f_{(i,j),(u,v)}^{k}(t) \quad (4)$$

The acceleration of an agent is calculated as in equation (5). Due to Newton's laws of motion, the acceleration of an agent is proportional to the resultant force and inverse of its mass [20]. Mass of i,j-th agent at the iteration t is represented as $M_{i,j}(t)$.

$$a_{i,j}^{k}(t) = \frac{F_{i,j}^{k}(t)}{M_{i,j}(t)} \quad (5)$$

The mass of agents is calculated with equation (6). α and ρ are constant values, which we have set to value of 0.1 for each.

$$M_{i,j}(t) = \alpha + \rho \times B_{i,j}(t) \quad (6)$$

Figure 2 illustrates the visual concept of applying the magnetic force on particles using equation (1) to enforce them move towards a specified direction (towards the highest index of features in data instance i). Using this concept, the IDS will act accurately in identifying the attack using our proposed algorithm, which forces its searching vector towards the most attractive set of features that classifies a particular type of attack. As we can see from Figure 2, the average electromagnetic force increases proportionally to the number of masses. The more masses we have, the higher the average electromagnetic force between them due to the attraction and repulsion forces between them. This results in higher exploration of the search space of IDS.

The position of agents and velocity are updated and calculated as in equation (7) and equation (8). *rand* is a random number in the interval [0,1]. In MOA, all agents are initialized with random values.

$$v_{i,j}^{k}(t+1) = rand \times v_{i,j}^{k}(t) + a_{i,j}^{k}(t) \quad (7)$$

$$x_{i,j}^{k}(t+1) = x_{i,j}^{k}(t) + v_{i,j}^{k}(t+1) \quad (8)$$

The steps will continuously run until meeting an end condition. Magnetic fields and masses for all agents are defined

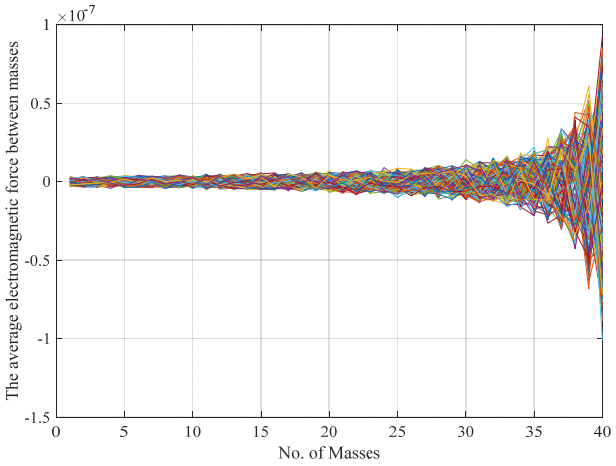

FIGURE 2. The average electromagnetic force presentation of the range of 0-40 masses applied using the equation (1).

using equations (3) and (6). After that, total forces of agents and accelerations are calculated as in equations (4) and (5). The velocities and positions of agents are updated using equations (7) and (8) [11].

Mean Squared Error (MSE): The mean squared error is a network performance function that measures how close a fitted line is to the data points [20]. In this work, the mean squared error is calculated as the average of the squares of the errors (deviations) for n number of trainings as in equation (9):

$$E_k = \frac{(o_i^k - d_i^k)^2}{n} \quad (9)$$

In equation (9), o_i^k is the actual output of the ith input unit when kth training sample is used and d_i^k is the desired output of the ith input unit when kth training sample is used. Equation (10) is used to calculate the final fitness which is the summation of all training MSE samples. Q stands for the number of training samples.

$$Fitness = \sum\nolimits_{k=1}^{Q} E_k \quad (10)$$

B. PROPOSED IDS BASED ON HYBRID MOA-PSO

The method proposed in this paper is for training ANN as a way to optimize the performance of IDS for better attack classification process. This is achieved via the hybridization of MOA and PSO to overcome the issues that normally are faced by the machine learning techniques like; entrapment in local minima, convergence speed, and sensitivity to initialization. First, we divide the dataset into two data sections for training 80% and testing 20% as presented in Figure 3 (the general process flow). Then, we develop a standard dataset format for the purpose of reorganization by ANN. Subsequently, when the training of the ANN has finished, the ANN starts its process in classifying the KDD CUP '99 testing dataset and takes the accurate outputs of the IDS's detection [30]. Then, all these steps are recorded and monitored as a way to improve

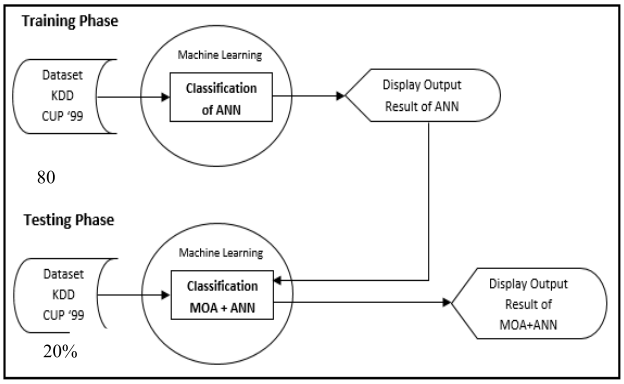

FIGURE 3. General process flow.

the system after n iterations. When the recognition phase of the ANN is over, at that stage, the ANN reorganization would be attempted to be optimized by our proposed hybrid MOA-PSO algorithm.

When the results of the ANN are optimized by our proposed hybrid MOA-PSO algorithm, they will be compared with the ANN results with and without MOA as well as PSO and GA algorithms, so that the effects of MOA could be more investigated in the ANN reorganization in the field of IDS with the KDD CUP dataset. To support ANN in IDS optimization, the PSO is implemented in this paper. PSO is used in this paper by hybridizing it with MOA to support ANN during IDS's attack recognition process.

It is good to note that KDD CUP dataset has been widely used by the researchers, especially for IDS studies and this database contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment. Moreover, it is quite difficult to collect such huge amount of data with a Lab's set-up environment to obtain long-term raw TCP dump data for a network. The network was operated as if it were a real environment, but sprinkled with multiple attacks. We have contributed here is that using the same structure of KDD Cup dataset's attributes, we collected some more network traffic instances via the conducted scenario as shown in Figure 1, to be added into KDD CUP dataset.

The information is further processed with the final weights to obtain a value in the output layer of the ANN. Based on the output obtained; further classification of the presence of any intrusion is done. Figure 4 shows the flowchart of IDS using hybrid MOA-PSO. When the traffic instance is classified as anomaly, further analysis should take place as a way to identify the main features that indicate a particular type of attack. Thus, our proposed hybrid MOA-PSO addresses this point via analyzing the index value of each feature as presented by f_i in sub-section A under Section III.

Information Gain has been widely employed as a robust benchmark in the area of machine learning [31]. Thus, the extracted features using the tagged index values will represent the information gain to be used as a base for IDS detection procedure. In other words, our algorithm

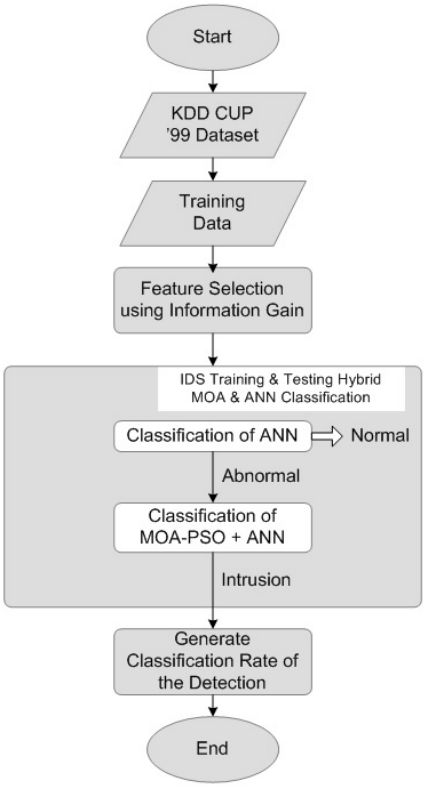

FIGURE 4. Flowchart of proposed IDS based on hybrid MOA-PSO algorithm.

employs a normalized information gain benchmark to nominate attributes from a given set of attributes as a way to adjust the splitting point. Our information gain will inspect each feature in isolation, calculate its information gain and evaluate how significant its correlation to the class label (attack type). During the process of information gain calculation for each feature, the entropy of the categorized class (attack type) will be calculated for the complete dataset isolating the uncertain entropies for each potential value of a particular feature. This process requires a frequent calculation of the categorized class via feature value. In more precise form, all occurrences (attacks) are nominated with some feature value f_i, then the number of incidents of each attack category within these occurrences and the entropy of f_i are calculated.

Figure 5 demonstrates the coded procedure that was used in updating the fitness value of magnetic swarms in the search space using equations (1) and (2). In every iteration i, the weight value for each node would be updated according to the calculated mass's fitness value. When a particle has high index value, it indicates that the particle has high magnetic field compared with others. So, this particle would be moving in a heavy form making the search deeper in that data instance looking for the local best solution. On the other hand, other particles with relatively lesser magnetic forces will be moving in a faster way looking for the global best solution. Thus, our proposed algorithm would be more accurate as it falls more or less in the global/local minima.

Initialize fitness values of particles
best=min(CurrentFitness)
worst=max(CurrentFitness)
for *all masses i<= n* **do**
Update the mass$_i$ value according to new obtained fitness value
Update the velocity value of mass$_i$ according to new mass volume
end for
Compute Magnetic force of each mass in the searching space
for *all masses i<= n* **do**
if *position mass$_i$ ≠ position mass$_{i-1}$* **then**
Calculate and Update the magnetic force of mass$_i$ using Eq. 1&2
end if
end for

FIGURE 5. Pseudocode of updating the fitness value of proposed IDS based on hybrid MOA-PSO.

C. STATISTICAL ANALYSIS OF UPDATED KDD CUP DATASET AND SAMPLE EXTRACTION

The Updated KDD CUP dataset has been used to supply the input values of our hybrid MOA-PSO technique. There are 41 features and 494020 records in the KDD CUP '99 dataset [32]. We have utilized the MLP's range of data to be either [0 1]. It is also important mentioning that each record of KDD CUP '99 is formed as continuous, discrete and symbolic, as presented in Table 2. In order to transform symbols into numerical form, an integer code has been given to each symbol. In other words, as a way to obtain an equal weight for all features, it is important to transform all of them under one main scale. Hence, all datasets were normalized as a step prior to the training process. In this regard, we have applied the Min-Max normalization, which can be defined as in equation (11), where $f_{normlized}$ is the normalized feature, f_{min} and f_{max} are the minimum and maximum values respectively, of the corresponding feature, $f_{normlized}$. Utilizing this equation, all features are scaled to the interval [0,1]. Moreover, in our work, four critical features of the dataset are selected of input values have been used to train the proposed hybrid MOA-PSO algorithm.

$$f_{normlized} = \frac{f_i - f_{min}}{f_{max-f_{min}}} \tag{11}$$

A population statistics was applied on selected samples for training and testing/validation of KDD CUP collected datasets to ensure that they are slightly different from that of the overall data. Besides, the training sample was selected whereby it contains all possible features used in identifying Smurf/Neptune types of attacks. The following formula shows the probability form of arbitrary data sample selection of feature f. Here, S_P is the population size and C_{n_i} is the number of combinations from S_P.

$$p_i = \frac{\left|C_{N_i,S_P}\right|}{|S_P|} \tag{12}$$

TABLE 2. Description of features based on KDD CUP dataset.

No.	Feature name	Description	Type
1	Duration	Length of the connection (second)	Continuous
2	Protocol_type	Type of protocol, e.g. tcp, udp, etc.	Discrete
3	Service	Network service on the destination, e.g., http, telnet, etc.	Discrete
4	Flag	Normal or error status of the connection	Discrete
5	Src_bytes	Number of data bytes from source to destination	Continuous
6	Dst_bytes	Number of data bytes from destination to source	Continuous
7	Land	1 if connection is from/to the same host/port; 0 otherwise	Discrete
8	Wrong_fragment	Number of ''wrong'' fragments	Continuous
9	Urgent	Number of urgent packets	Discrete
10	Hot	Number of ''hot'' indicators	Discrete
11	Num_failed_logins	Number of failed login attempts	Discrete
12	Logged_in	1 if successfully logged in; 0 otherwise	Discrete
13	Num_compromised	Number of compromised condition	Discrete
14	Root_shell	1 if root shell is obtained; 0 otherwise	Discrete
15	Su_attempted	1 if ''su root'' command attempted; 0 otherwise	Discrete
16	Num_root	Number of ''root'' accesses	Discrete
17	Num_file_creations	Number of file creation operations	Discrete
18	Num_shells	Number of shell prompts	Discrete
19	Num_access_files	Number of operations on access control files	Discrete
20	Num_outbound_cmds	Number of outbound commands in an ftp session	Discrete
21	Is_host_login	1 if the login belongs to the ''hot'' list; 0 otherwise	Discrete
22	Is_guest_login	1 if the login is a ''guest''login; 0 otherwise	Discrete
23	Count	Number of connections to the same host as the current connection in the past two seconds	Discrete
24	Srv_count	Number of connections to the same service as the current connection in the past two seconds	Discrete
25	Serror_rate	% of connections that have ''SYN'' errors	Discrete
26	Srv_serror_rate	% of connections that have ''SYN'' errors	Discrete
27	Rerror_rate	% of connections that have ''REJ'' errors	Discrete
28	Srv_rerror_rate	% of connections that have ''REJ'' errors	Discrete
29	Same_srv_rate	% of connections to the same services	Discrete
30	Diff_srv_rate	% of connections to different services	Discrete
31	Srv_diff_host_rate	% of connections to different hosts	Discrete
32	Dst_host_count	Count for destination host	Discrete
33	Dst_host_srv_count	Srv_count for destination host	Discrete
34	Dst_host_same_srv_rate	Same_srv_rate for destination host	Discrete
35	Dst_host_diff_srv_rate	Diff_srv_rate for destination host	Discrete
36	Dst_host_same_src_port_rate	Same_src_port_rate for destination host	Discrete
37	Dst_host_srv_diff_host_rate	Diff_host_rate for destination host	Discrete
38	Dst_host_serror_rate	Serror_rate for destination host	Discrete
39	Dst_host_srv_serror_rate	Srv_serror_rate for destination host	Discrete
40	Dst_host_rerror_rate	Rerror_rate for destination host	Discrete
41	Dst_host_srv_rerror_rate	Srv_serror_rate for destination host	Discrete

D. PARAMETER SETTING

Table 3 lists the parameter values of conducted simulation in this study (using MATLAB tool). We have conducted the experiments on four different sets of Masses/Particles, (10, 20, 30 and 40) with 25 nodes in the considered WANET. 3 malicious nodes have been assigned randomly to trigger the Smurf and Neptune attacks to testify the accuracy as well as the computational complexity during the learning and testing processes of ANN. The IDS would make use of the proposed

TABLE 3. Simulation parameters.

Simulation Parameter	Assigned Values
Total no. of nodes	25
No. of malicious nodes	3
Mass/Particles	Four sets, 10, 20, 30 and 40
Maximum of Iteration	500
Number of Training Samples	200
Inertia Weight	2
Minimum weight	0.5
Maximum weight	0.9
Max Velocity	5
α	0.1
ρ	0.1
Objective Function	Maximize the classification rate & Minimization of MSE

hybrid MOA-PSO as well as the other benchmark algorithms to extract the sub-set of features that mostly indicate the Smurf/Neptune types of attacks, which would be used afterwards in the classification process. In spite of other settings, the predefined objective function in this study is set up to maximize the classification rate of our proposed mechanism and at the same time minimize the average MSE.

IV. RESULTS AND DISCUSSION

In this section, the obtained results from our experiments have been collected and discussed. Moreover, as a way to validate the performance of our proposed IDS, we have compared the results with other representatives of IDS based on machine learning systems. It should be noted that the reported classification rates in this section were obtained as an average of statistical analysis that was performed during the training and testing phases after every iteration out of 10 runs. Moreover, in the following sub-sections *A* and *B*, the simulation results are gathered and discussed using different sets of extracted features and different parameters such as, number of particles in PSO, number of masses in our proposed IDS, number of agents using other compared algorithms. The performance analysis was conducted with different scenarios to achieve fair performance evaluation. The following sub-sections elaborate the performance evaluation and validation of our proposed approach.

A. RELEVANT FEATURE SELECTION

In our work, four critical features have been selected to classify the Smurf and Neptune types of attacks compared with normal activities in IDS. The performance analysis has been conducted to compare our proposed IDS based on hybrid MOA-PSO in terms of the classification rate with other best feature selection techniques that use PSO, GA and MOA/GSA [20]. Table 4 lists the most relevant features that widely have been used in IDS classifications based on KDD CUP '99 dataset [20]. Table 5 lists the extracted and elaborated features in this work in the classification process for each of the traffic representing Normal, Smurf Attack, and Neptune Attack. Figure 6 demonstrates the pseudocode of calculating classification rate of IDS, whereby three classes are defined and labeled as −1 for Smurf attack, 1 Neptune attack and 0 for normal traffic. It is important highlighting that the features presented in Table 5 have been obtained and benchmarked based on conducted literature as well as training and analysis phases using our proposed algorithm, which has shown that these features are more likely the related indicators for each of Normal, Smurf Attack, and Neptune attack traffics. For more detailed understanding, we refer the reader to Table 2, where the description of each feature is listed.

TABLE 4. Most relevant features.

Work	Relevant Features
[7]	3, 5, 29 and 39
	36, 37, 38 and 39
	3, 6, 29 and 30
[20]	3, 23, 30 and 36

TABLE 5. Relevant features for normal, Smurf attack and neptune attack (Olusola *et al*, 2010) [21].

Class Label	Relevant Features
Normal	3,6,12,23,25,26,29,30,33,34,35,36,37,38,39
Smurf	2,3,5,6,12,25,29,30,32,36,37,39
Neptune	3,4,5,23,26.29,30,31,32,34,36,37,38,39

```
Initiate ClassificationRate, Weight, Biases values, TrainingNo
Smurf = -1, Neptune = 1, Normal = 0
while TrainingNo <= n do
Update the mass_i value according to new obtained fitness value
Update the velocity value of mass_i according to new mass volume
Calculate the Target_Value_n of classification Smurf/Neptune/Normal
  if Target_Value_n = -1 then
        ClassificationRate = ClassificationRate + 1
  end if
  if Target_Value_n = 1 then
        ClassificationRate = ClassificationRate + 1
  end if
  if Target_Value_n = 0 then
        ClassificationRate = ClassificationRate + 1
  end if
end while
ClassificationRate = (ClassificationRate/ TrainingNo) * 100
Return ClassificationRate
```

FIGURE 6. Pseudocode of calculating classification rate of IDS.

B. FEATURE SELECTION AND CLASSIFICATION OF THE PROPOSED IDS

Figure 7 illustrates the classification rates. The highest classification rate using our proposed IDS based on hybrid MOA-PSO with the best features 3, 5, 29 and 36, was 98.50%. The second highest was with the features 3, 5, 29 and 39 that could produce 97.50% classification rate. Feature number 36 is very important since it influenced the rate of classification. Feature 39 is represented as Destination Host Name Source Port Rate, which could give a good indicator about the types of activities (whether it is Normal, Smurf attack, or Neptune attack).

On the other hand, Figure 8 shows the MSE of our proposed mechanism using the best selected features: 3, 5, 29, and 36. We can observe the efficiency of our proposed IDS in obtaining zero or closer to zero of MSE value right after 30 iterations of training. Therefore, we have decided to utilize the set of features: 3, 5, 29 and 36 as the main indicators in classifying the WANET traffic as Normal, Smurf attack, or Neptune attack. Figure 9 shows the comparison between our proposed detection method and IDS based on MOA, PSO and GA. The simulation experiments were run using the most relevant features: 3, 5, 29 and 36 that

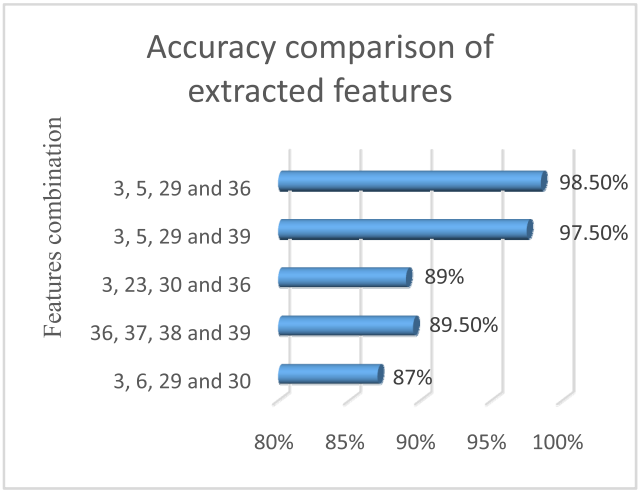

FIGURE 7. Performance of the proposed IDS based on hybrid MOA-PSO in finding the best collection of dataset features in classifying Normal, Smurf attack, Neptune attack network traffic.

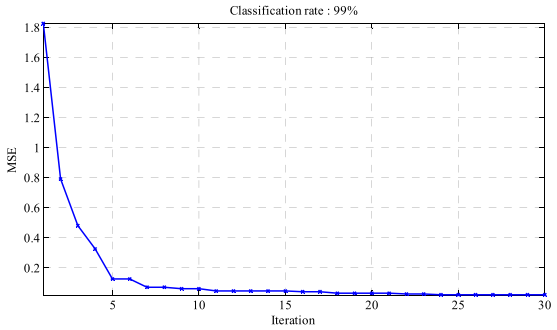

FIGURE 8. MSE of proposed mechanism using features 3, 5, 29 and 36.

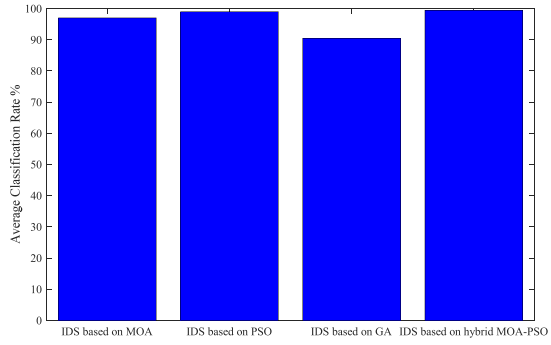

FIGURE 9. Comparison between MOA, PSO, GA and proposed IDS based on hybrid MOA-PSO using features 3, 5, 29 and 36.

are extracted. We can observe that our mechanism could maintain high classification rate represented by 99.5%. In other words, our proposed IDS could achieve 0.5% improvement using selected features 3, 5, 29 and 36 in comparison with its counterparts based on MOA and PSO.

C. OPTIMIZING DIFFERENT SETS OF IDS PARAMETERS

Based on the concept that we have introduced previously in [20], the efficiency of agents depends on the masses. In other words, the heavier masses are more efficient agents; which means that they have relatively higher attraction force. Thus, lower masses are not efficient agents. However, we should not ignore the fact that higher masses take a long time than the lower masses to search in the population. Therefore, in this section, the results are compared and discussed using different sets of parameter settings as a way to find the best set that could offer the highest accuracy level.

In order to find out the most suitable set of parameters to be used in optimization, we have studied the performance of our proposed IDS based on hybrid MOA-PSO along with its representatives with three different sets of masses/particles. Figures 10(a), 10(b) and 10(c) show the MSE values achieved during simulating our technique in classifying types of network traffic. We have found that use of 20 and 30 masses have showed 97% and 99% of IDS classification accuracy, respectively while it was improved to 99.5% when the number of masses was increased to 40 masses. The reason is that more number of masses plays an effective role in improving the performance of our proposed IDS in finding the accurate detection rate. It is also important to note that increasing the number of masses increases the computational cost since the algorithm needs to count the gravity function value for each particular mass. Thus, the intention of using high or low number of masses is subject to the objective function that could be defined early by IDS's policy.

Therefore, in this work, we have found that the more suitable parameter settings to be used are; masses equal to 30, 500 as the maximum number of iterations, 15 nodes in the hidden layer, 200 training samples, and 2 for inertia weight. Figure 11 illustrates a comparison of the accuracy values of our proposed hybrid MOA-PSO against MOA, PSO and GA algorithms in IDS. We can observe that with different parameter settings, our proposed hybrid MOA-PSO performance is the best. Our proposed method could achieve high detection rate and high classification rate with low iteration numbers and masses

The previous classification rate results shown in Figure 11 that were achieved by implementing our proposed hybrid MOA-PSO optimization on ANN have achieved 99% while Figure 12 presents the results obtained using the most relevant features 3, 5, 29 and 36 from KDD CUP Dataset (compared with our proposed IDS). The testing process using the same selected features on PSO, GA and MOA in optimizing ANN has been applied to testify the accuracy of our proposed IDS based on MOA-PSO. It is important to remind the readers that we have applied the same parameter setting as discussed in subsection c. The detailed results shown in Figure 12(a) are obtained based on MOA optimization with ANN, which has produced 98.5% accuracy. It is proven that MOA optimization on ANN performs better than PSO optimization on ANN (i.e., for better performance of IDS). The simulations were executed with 30 particles and 500 iterations. Similarly, the experiment was conducted using PSO technique with the same features; the obtained accuracy was improved to 97.5% as demonstrated in Figure 12(b). On the other hand, we have utilized GA algorithm to benchmark

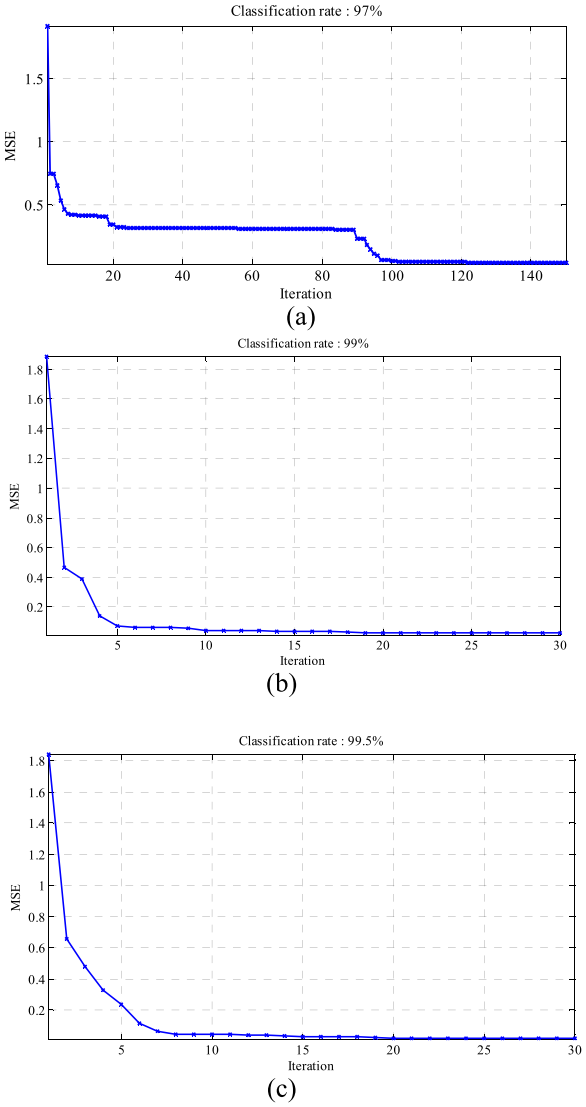

FIGURE 10. (a) Optimizing ANN with Hybrid MOA- PSO using masses 20; (b) ANN optimized by Hybrid MOA- PSO using masses 30; (c) ANN optimized by Hybrid MOA-PSO using masses 40.

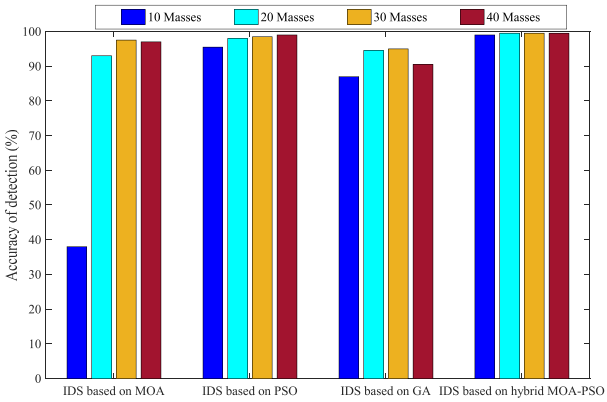

FIGURE 11. Comparison of Masses/Agents 10, 20, 30 and 40 of MOA, PSO, GA and Hybrid MOA-PSO.

the performance and we have observed the classification rate was within the average of 91% with 30 population size as presented in Figure 12(c).

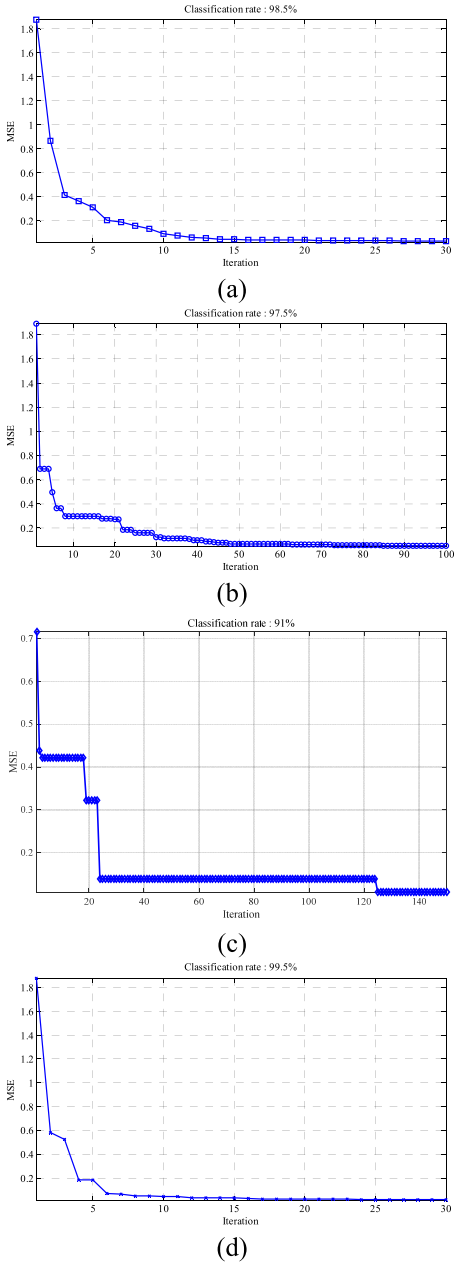

FIGURE 12. (a) Result of ANN optimized by MOA; (b) Result of ANN optimized by PSO; (c) Result of ANN optimized by GA; and (d) Result of proposed IDS based on hybrid MOA-PSO using the same set of features 3, 5, 29 and 36.

We have also conducted experiments with the same aforementioned simulation settings to apply our proposed IDS with the same data features. The classification rate achieved 99.5% accuracy. It is worth highlighting that our proposed mechanism could achieve this high level of accuracy with the earliest 100 iterations. This indicates that our proposed IDS is more efficient in the attack's classification process. Figure 12(d) shows the result of our proposed mechanism.

Finally, Figure 13 shows the graph plots of the compared results for each of PSO, MOA, GA and our proposed IDS. The comparison is accompanied with the level of

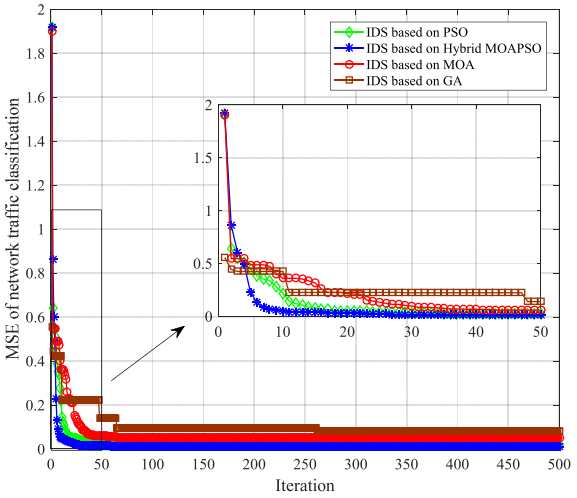

FIGURE 13. Comparison among MOA, PSO, GA and our proposed IDS based on hybrid MOA-PSO using 40 Masses/Pericles.

classification accuracy rates. Function approximation has 200 training a sample, thus the findings out of the KDD CUP Dataset confirm that our proposed IDS is performing good with large number of training samples with less number of iterations. Long story short, presented results have verified that our proposed IDS based on hybrid MOA-PSO has better performance than the ones based on PSO, MOA and GA for high training sample and the most relevant dataset features to classify the attacks in IDS.

V. CONCLUSIONS AND FUTURE WORKS

In this paper, an efficient IDS based on hybrid MOA-PSO is proposed. An updated KDD CUP dataset is used to represent the different types of WANET traffics, which is a collection of normal and attack traffic. The proposed mechanism has been implemented and simulated using MATLAB toolkit. The conducted steps of the proposed methodology in this study were focused on training and testing based on KDD CUP dataset, with finally selecting four critical features that we used for intrusion detection. Two WANET attack categories have been used for training our proposed mechanism, which are Smurf and Neptune. Also, the ability of the proposed IDS in classifying the WANET traffic (whether it is normal or abnormal) has been tested. Our mechanism has shown performance with higher accuracy and efficiency than other available alternatives approaches. The results have shown that our proposed IDS based on hybrid MOA-PSO could achieve high classification rate up to 99.5% while IDS based on only PSO has obtained 97.5% and IDS based on MOA could maintain 99%. Using GA based IDS, the detection accuracy was 95% as the maximum obtained average rate.

As future work, we intend to evaluate our mechanism with more types of attacks to validate the classification as well as detection's percentage under dynamic settings. We are also currently planning to improve our proposal to construct a sensitive model to be integrated with our IDS for attack detection.

REFERENCES

[1] F. Haddadi and M. A. Sarram, "Wireless intrusion detection system using a lightweight agent," in *Proc. 2nd Int. Conf. Comput. Netw. Technol. (ICCNT)*, 2010, pp. 84–87.
[2] A.-S. K. Pathan *et al.*, "Defending against wireless network intrusion," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 499–501, 2014.
[3] A.-S. K. Pathan, *The State of the Art in Intrusion Prevention and Detection*. Boca Raton, FL, USA: CRC Press, 2014.
[4] S. Khan, A.-S. K. Pathan, and N. A. Alrajeh, *Wireless Sensor Networks: Current Status and Future Trends*. Boca Raton, FL, USA: CRC Press, 2016.
[5] S.-J. Horng *et al.*, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert Syst. Appl.*, vol. 38, no. 1, pp. 306–313, 2011.
[6] A. Derhab, A. Bouras, M. R. Senouci, and M. Imran, "Fortifying intrusion detection systems in dynamic ad hoc and wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 12, p. 608162, 2014.
[7] Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, "An efficient intrusion detection system based on support vector machines and gradually feature removal method," *Expert Syst. Appl.*, vol. 39, no. 1, pp. 424–430, 2012.
[8] B. Al-Dhafian, I. Ahmad, M. Hussain, and M. Imran, "Improving the security in healthcare information system through elman neural network based classifier," *J. Med. Imag. Health Informat.*, vol. 7, no. 6, pp. 1429–1435, 2017.
[9] A. A. Ahmed, "Investigation model for DDoS attack detection in real-time," *Int. J. Softw. Eng. Comput. Syst.*, vol. 1, no. 1, pp. 93–105, 2015.
[10] K. S. Desale, C. N. Kumathekar, and A. P. Chavan, "Efficient intrusion detection system using stream data mining classification technique," in *Proc. Int. Conf. Comput. Commun. Control Autom. (ICCUBEA)*, 2015, pp. 469–473.
[11] S. Mirjalili and A. S. Sadiq, "Magnetic optimization algorithm for training multi layer perceptron," in *Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2011, pp. 42–46.
[12] A. A. Ahmed, A. S. Sadiq, and M. F. Zolkipli, "Traceback model for identifying sources of distributed attacks in real time," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2173–2185, 2016.
[13] S. Khan, A. Gani, A. W. A. Wahab, and P. K. Singh, "Feature selection of denial-of-service attacks using entropy and granular computing," *Arabian J. Sci. Eng.*, vol. 43, no. 2, pp. 499–508, 2018.
[14] D. H. Wolper and W. G. Macready, "No free lunch theorems for optimization," *IEEE Trans. Evol. Comput.*, vol. 1, no. 1, pp. 67–82, Apr. 1997.
[15] W. Tian and J. Liu, "A new network intrusion detection identification model research," in *Proc. 2nd Int. Asia Conf. Inf. Control, Autom. Robot. (CAR)*, 2010, pp. 9–12.
[16] S. Mirjalili, A. Lewis, and A. S. Sadiq, "Autonomous particles groups for particle swarm optimization," *Arabian J. Sci. Eng.*, vol. 39, no. 6, pp. 4683–4697, 2014.
[17] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," *Procedia Comput. Sci.*, vol. 19, pp. 1101–1107, Jan. 2013.
[18] Q. S. Qassim, A. M. Zin, and M. J. A. Aziz, "Anomaly-based network IDS false alarm filter using cluster-based alarm classification approach," *Int. J. Secur. Netw.*, vol. 12, no. 1, pp. 13–26, 2017.
[19] O. A. Mahdi *et al.*, "A comparison study on node clustering techniques used in target tracking WSNs for efficient data aggregation," *Wireless Commun. Mobile Comput.*, vol. 16, no. 16, pp. 2663–2676, 2016.
[20] A. Dastanpour, S. Ibrahim, R. Mashinchi, and A. Selamat, "Using gravitational search algorithm to support artificial neural network in intrusion detection system," *SmartCR*, vol. 4, no. 6, pp. 426–434, 2014.
[21] A. A. Olusola, A. S. Oladele, and D. O. Abosede, "Analysis of KDD'99 intrusion detection dataset for selection of relevance features," in *Proc. World Congr. Eng. Comput. Sci.*, 2010, pp. 20–22.
[22] R. Entezari-Maleki, M. Gharib, M. Khosravi, and A. Movaghar, "IDS modelling and evaluation in WANETs against black/grey-hole attacks using stochastic models," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 27, no. 3, pp. 171–186, 2018.
[23] A.-S. K. Pathan and C. S. Hong, "SERP: Secure energy-efficient routing protocol for densely deployed wireless sensor networks," *Ann. Telecommun.-Ann. Télécommun.*, vol. 63, nos. 9–10, pp. 529–541, 2008.
[24] M. K. Khan, M. Shiraz, K. Z. Ghafoor, S. Khan, A. S. Sadiq, and G. Ahmed, "EE-MRP: Energy-efficient multistage routing protocol for wireless sensor networks," *Wireless Commun. Mobile Comput.*, Jan. 2018, Art. no. 6839671, doi: 10.1155/2018/6839671.

[25] I. Yaqoob *et al.*, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Netw.*, vol. 129, pp. 444–458, Dec. 2017.
[26] C.-F. Chao and M.-H. Horng, "The construction of support vector machine classifier using the firefly algorithm," *Comput. Intell. Neurosci.*, Jan. 2015, Art. no. 2, doi: 10.1155/2015/212719.
[27] G. Chandrashekar and F. Sahin, "A survey on feature selection methods," *Comput. Elect. Eng.*, vol. 40, no. 1, pp. 16–28, Jan. 2014.
[28] M. M. Mohammed, H. A. Chan, N. Ventura, and A.-S. K. Pathan, "An automated signature generation method for zero-day polymorphic worms based on multilayer perceptron model," in *Proc. Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT)*, 2013, pp. 450–455.
[29] F. Haddadi and A. N. Zincir-Heywood, "Benchmarking the effect of flow exporters and protocol filters on botnet traffic classification," *IEEE Syst. J.*, vol. 10, no. 4, pp. 1390–1401, Dec. 2016.
[30] S. Anwar *et al.*, "From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 39, 2017.
[31] Y. Yang and J. O. Pedersen, "A comparative study on feature selection in text categorization," in *Proc. ICML*, 1997, pp. 412–420.
[32] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skoric, "Towards an information-theoretic framework for analyzing intrusion detection systems," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2006, pp. 527–546.

ALI SAFAA SADIQ (M'16) received the B.Sc., M.Sc., and Ph.D. degrees in computer science in 2004, 2011, and 2014, respectively. He is currently a Faculty Member with the School of Information Technology, Monash University, Malaysia. His current research interests include intelligent handover decision making in heterogeneous wireless networks, vehicular and mobile ad hoc networks, artificial intelligent applications in computer networks, energy efficient routing protocols, wireless sensor networks, media access control layer design, mobile IPV6 and video communications, developing smart intrusion detection systems, forecasting & decision making techniques, and cognitive vehicular networks. He could secure three research grants as well as joining few other funds under ministry of higher education in Malaysia. During his academic career, he has supervised six Postgraduate students and published several scientific/research papers in well-known international journals and conferences in additional to international books in the field his research.

BASEM ALKAZEMI is currently an Associate Professor with the College of Computer and Information System, Umm Al-Qura University, Saudi Arabia. He is also the Head of the Software Engineering Research Group, Umm Al-Qura University, and also holding the position of Vice Dean for Research Projects and Grants in the deanship of scientific research. His current research interests include software engineering and data mining. He is involved, as a PI, in a number of funded research projects in the area of WSN, Bigdata, and NLP. He served as a reviewer in several international conferences and journals. He supervised four master students those conducted their thesis in software continuous delivery (CD), BPM, IoT, and Bigdata for retails.

SEYEDALI MIRJALILI received the Ph.D. degree in computer science from Griffith. He is currently a Lecturer with Griffith University. His research interests include robust optimisation, engineering optimisation, multi-objective optimisation, swarm intelligence, evolutionary algorithms, and artificial neural networks. He is involved in the application of multi-objective and robust meta-heuristic optimisation techniques in computational fluid dynamic problems as well. He is internationally recognised for his advances in swarm intelligence (SI) and optimization, including the first set of SI techniques from a synthetic intelligence standpoint a radical departure from how natural systems are typically understood and a systematic design framework to reliably benchmark, evaluate, and propose computationally cheap robust optimisation algorithms. He has published over 70 journal articles, many in high-impact journals. He has over 4000 citations in total with an H-index of 24 and G-index of 63. From Google Scholar metrics, he is globally the third most cited researcher in Engineering Optimization and Robust Optimization.

NORAZIAH AHMED received the B.Sc. degree from the Universiti Putra Malaysia, Certificate in teaching and learning from Northern Illinois University, USA, and the Ph.D. from Universiti Malaysia Terengganu. She is currently an Associate Professor with the Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang. Her current research interests are distributed databases, data grid and data mining, computational intelligence, cloud computing, and big data analytic.

SULEMAN KHAN received several Master programs, including the M.Sc. degree in computer science from the University of Peshawar, Pakistan, in 2006, the M.B.A. degree in HRD from the Institute of Management of Sciences, Hayatabad, Pakistan, in 2007, and the M.S. degree in distributed systems from the Comsats Institute of Information Technology, Abbottabad, Pakistan, in 2011, and the Ph.D. degree (Hons.) from the Faculty of Computer Science and Information Technology, University of Malaya, Malaysia, in 2017. He is currently a Lecturer with the School of Information Technology, Monash University, Malaysia. He has published 40 High Impact Research articles in reputed international journals and conferences. His research areas include but are not limited to network security, network forensics, software defined networks, Internet of Things, cloud computing, and vehicular communications.

IHSAN ALI received the M.Sc. degree from Hazara University Manshera, Pakistan, in 2005, and the M.S. degree in computer system engineering from the GIK Institute in 2008. He is currently pursuing the Ph.D. degree with the Faculty of Computer Science and Information Technology, University of Malaya. He has over five year teaching and research experience in different country, including Saudi Arabia, USA, Pakistan, and Malaysia. He has published over 10 papers in the international journals and conferences His research interests include wireless sensor networks, underwater sensor network, sensor cloud, fog computing, and IOT. He has served as a Technical Program Committee Member for the IWCMC 2017, AINIS 2017, Future 5V 2017, and also an organizer of Special session on fog computing in Future 5V 2017. He is also a reviewer of *Computers & Electrical Engineering*, *KSII Transactions on Internet and Information Systems*, *Mobile Networks and Applications*, the *International Journal of Distributed Sensor Networks*, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Computer Networks, the IEEE ACCESS, and the *IEEE Communication Magazine*.

AL-SAKIB KHAN PATHAN received the B.Sc. degree in computer science and information technology from the Islamic University of Technology, Bangladesh, in 2003, the Ph.D. degree (M.S. leading to Ph.D.) in computer engineering from Kyung Hee University, South Korea, in 2009. He was an Assistant Professor with the Faculty of Computer and Information Systems, Islamic University of Madinah, Medina, Saudi Arabia. He is currently an Associate Professor with the Department of Computer Science and Engineering, Southeast University, Dhaka, Bangladesh. His research interests include wireless sensor networks, network security, and e-services technologies. He is currently involving in some multidisciplinary issues. He was a recipient of several awards/best paper awards and has over 170 publications in these areas. He has served as a chair, organizing committee member, and technical program committee member in numerous international conferences/workshops like GLOBECOM, ICC, GreenCom, AINA, WCNC, HPCS, ICA3PP, IWCMC, VTC, and HPCC. He received the IEEE Outstanding Leadership Award and the Certificate of Appreciation for his role in IEEE GreenCom'13 Conference. He is currently serving in various editorial positions like as an Associate Technical Editor for the *IEEE Communications Magazine*, an Editor for the *Ad Hoc and Sensor Wireless Networks*, Old City Publishing, and the *International Journal of Sensor Networks*.

KAYHAN ZRAR GHAFOOR received the B.Sc. degree in electrical engineering from Salahaddin University, the M.Sc. degree in remote weather monitoring from Koya University, and the Ph.D. degree in wireless networks from the University Technology Malaysia in 2003, 2006, and 2011, respectively. He was a Visiting Researcher with the Faculty of Computing, University Technology Malaysia, for six months. He is currently serving as a Post-Doctoral Fellow with the School of Computer and Electrical Engineering, Shanghai Jiao Tong University, and a Faculty Member with the Department of Computer Science, Faculty of Science, Cihan University-Erbil, Erbil, Iraq. He has published over 50 scientific/research papers in ISI/Scopus indexed international journals and conferences. He has authored two books named *Cognitive Networks: Applications and Deployments* and *Privacy and Cybersecurity in Smartcities*. He was a TPC member for over 37 international conferences, including GlobCom and InfoCom. He was a recipient of the UTM Chancellor Award at 48th UTM convocation in 2012. He was a General Chair of a workshop named Smart Sensor Protocols and Algorithms under the 9th International Conference on Mobile Ad-hoc and Sensor Networks (2014) which is held in Hungary. He also served as an Associate Editor, an Editorial Board Member, and a reviewer for numerous prestigious international journals, appeared as a workshop general chair for international workshops and conferences.