A Study on Swarm Intelligence Techniques in Intrusion Detection

P.Amudha
Faculty of Engineering
Avinashilingam Institute for Home Science and Higher Education for Women
Coimbatore, Tamilnadu, India

H.Abdul Rauf Ph.D
MEA Engineering College
Perinthalmanna
Kerala, India

ABSTRACT

Intrusion Detection System is a security support mechanism which has received great attention from researchers all over the globe recently. In the recent past, bio-inspired meta-heuristic technique such as swarm intelligence is being proposed for intrusion detection. Swarm Intelligence approaches are used to solve complicated problems by multiple simple agents without centralized control. The swarm intelligence algorithms inspired by animal behaviour in nature such as ants finding shortest path in finding food; a flock of birds flies or a school of fish swims in unison, changing directions in an instant without colliding with each other has been successfully applied to optimization, robotics and military applications. But however, its application to the intrusion detection domain is limited but interesting and inspiring. This paper provides an overview of the research progress in swarm intelligence techniques to the problem of intrusion detection.

Keywords

Intrusion detection, bio-inspired, swarm intelligence, meta-heuristic.

1. INTRODUCTION

Network security has become an indispensable factor of computer technology with the development of internet. The security of a computer system or network is compromised when an intrusion takes place. An intrusion can be defined as any set of actions that makes an attempt to compromise the integrity, confidentiality or availability of a resource. Intrusion prevention techniques such as firewalls, access control or encryption have failed to fully protect networks and systems from increasing attacks and malwares. As a result, Intrusion Detection System (IDS) have become an essential component of security infrastructure to detect these threats, identify and track the intruders. As IDS must have a high attack Detection Rate (DR), with a low False Alarm Rate (FAR) at the same time, construction of IDS is a challenging task. In the recent past, biology inspired approaches have made their appearance in a variety of research fields, ranging from engineering, computer science, economics, medicine and social sciences. Likewise, many biology inspired techniques have been proposed for intrusion detection to improve their efficiency and performance. Swarm intelligence is one of them. Techniques and algorithms of this research field draw their inspiration from the behaviour of insects, birds and fishes, and their unique ability to solve complex tasks in the form of swarms.

This paper reviews the swarm intelligence techniques used by the researchers for improving the performance of intrusion detection model. The remainder of this paper is organized as follows: Section 2 provides an introduction to intrusion detection and dataset description. Section 3 gives an insight of swarm intelligence techniques used in intrusion detection and Section 4 gives conclusion.

2. INTRUSION DETECTION

Recently, Intrusion Detection System has received great attention from researchers all over the world because of their ability to keep track of the network behaviour, so that abnormal behaviour can be detected quickly. Figure 1 shows the intrusion detection model.

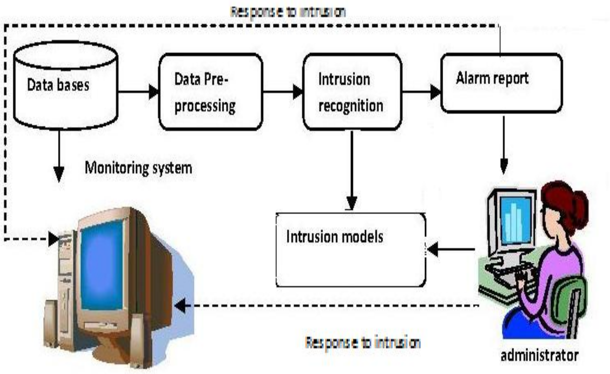

Figure 1. Intrusion Detection model

An IDS is generally categorized as misuse detection and anomaly detection. The misuse detection can detect intrusions with low false alarm rate, but it fails to detect new attacks. IDS analyze the information it gathers and matches with the large databases of intrusive behaviour or attack signatures. It is also known as signature-based detection. Anomaly detection has the capability of detecting new types of attacks and is classified as static and dynamic. It determines whether deviation from the established normal usage patterns and is stated as intrusions. The characteristics of intrusion detection system [38] are shown in Figure 2.

The two most popular performance evaluation metrics in IDS are: Detection Rate (DR), which is defined as the ratio of the number of correctly detected attacks to the total number of attacks, and False Alarm Rate (FAR), or False Positive Rate (FPR), which is the ratio of the number of normal connections that are misclassified as attacks to the total number of normal connections.

2.1 Intrusion Detection Dataset

The benchmark datasets commonly used by the researchers used in both misuse and anomaly detection are: DARPA 1998 TCPDump Files (DARPA98), DARPA 1999 TCPDump Files (DARPA99), KDDCUP99 dataset (KDDCUP99), 10% KDDCUP99 dataset (KDDCUP99-10), UNIX User dataset (UNIXDS), University of New Mexico dataset (UNM).

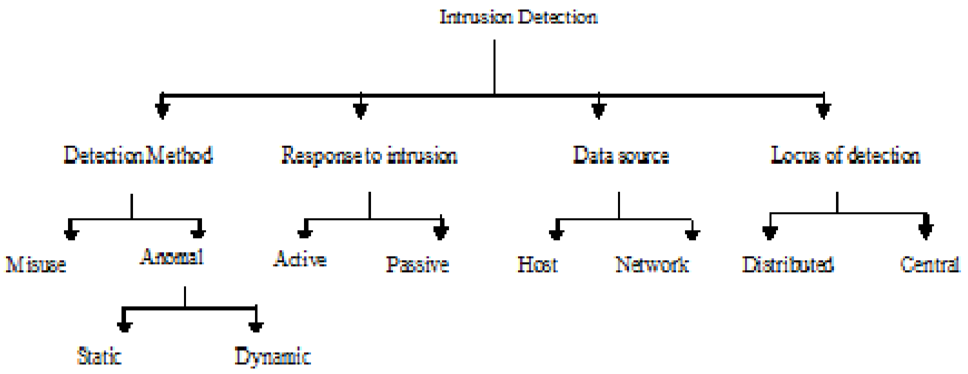

Figure 2. Characteristics of intrusion detection system

The widely used intrusion detection KDDCup99 dataset [22] which is focused in this paper was derived from the 1998 DARPA Intrusion detection Evaluation program prepared and managed by MIT Lincoln Laboratory. The dataset was a collection of simulated raw TCP dump data over a period of nine weeks of simulating a U.S. Air Force Local Area Network. It was operated like a real environment, but being blasted with multiple attacks. Seven weeks of training network traffic data was about four gigabytes of compressed binary TCP dump data which was processed into five million connection records. Similarly, two weeks of test data yielded about two million connection records. There are 4,898,430 labeled and 311,029 unlabeled connection records in the dataset and labeled connection records consist of 41 attributes.

In KDD99 dataset, each example represents attribute values of a class in the network data flow, and each class is labelled either normal or attack. The classes in KDD99 dataset are categorized into five main classes: one normal class and four main intrusion classes: *Denial of Service* (DoS), *Probe*, *User-to-Root* (U2R), *Remote-to-Login* (R2L).

- DoS attacks: use of resources or services is denied to authorized users.
- Probe attacks: information about the system is exposed to unauthorized entities.
- User to Remote attacks: access to account types of administrator is gained by unauthorized entities.
- Remote to Local attacks: access to hosts is gained by unauthorized entities.

The four attack classes (DoS, U2R, R2L, and probe) are divided into 22 different attack classes that are tabulated in Table 1.

Table 1. Detail of Attacks of Labeled Records

Category of attack	Attack Name
Normal	Normal
DoS	Neptune,Smurf,Pod,Teardrop,Land,back
Probe	Portsweep, IPsweep, Nmap, satan
U2R	Bufferoverflow,LoadModule,Perl,Rootkit
R2L	Guesspassword,Ftpwrite,Imap,Phf, Multihop,Warezmaster,Warezclient

The KDD99 intrusion detection benchmark dataset consists of three components namely: *10% KDD, Corrected KDD, Whole KDD* as shown in Table 2. In the International Knowledge Discovery and Data Mining Tools Competition, only *10% KDD* dataset was employed for the purpose of training and it is a more concise version of *Whole KDD* dataset. It contains more records of attacks than normal connections and the attack types are not distributed equally.

Table 2: Number of attacks in training KDDCUP'99 dataset

Dataset	Normal	DoS	U2R	R2L	Probe
10% KDD	97277	391458	52	1126	4107
Corrected KDD	60593	229853	70	11347	4106
Whole KDD	972780	3883370	50	1126	41102

3. BIO-INSPIRED APPROACHES

The techniques referred in Table 3 are typically used to solve search and optimisation problems, such as Genetic Algorithms (GAs) (Holland 1992, Goldberg 1989) [20][17], Genetic Programming (GP) (Koza 1992; 1994) [24][25], Particle Swarm Optimisation (PSO) (Kennedy and Eberhart 1995, Banks *et al.* 2008a; b)[23][6][7], and Ant Colony Optimisation (ACO) (Dorigo *et al.* 1999, Dorigo and Stutzle 2004)[13][14][15]. One of the strengths of these techniques is their parallel nature, and that their application is very diverse, provided that the problem can be quantified into some form of fitness measure.

Table 3. Bio-inspired approaches

Author	Year	Techniques proposed
Goldberg D. E.	1989	Genetic algorithm
John R.Koza	1994	Genetic Programming
Dorigo et al.	1999	Ant Colony Optimization
Kennedy and Eberhart	1995	Particle Swarm Optimisation

GAs and PSO are commonly associated with the optimisation of continuous numerical functions, and ACO with combinatorial optimisation. Some of the benefits of adopting such techniques are flexibility in retraining, online/continuous learning and the potential for parallelism in the algorithms, which can be exploited both in the training and detection process. However, the challenge is to represent the intrusion detection problem in a form that can be processed and evaluated by these algorithms. The techniques can be applied to intrusion detection as detectors.

Balajinath and Raghavan (2001) applied GA to perform intrusion detection based on UNIX commands. First, they encoded the commands with numeric values which were done in an ascending order according to the frequency of use. They then used user behaviour entropy indices as a measure of the randomness of the command history of each user, represented as a 3-tuple (match index; entropy index; newness index). The match index is "a measure of regularity in user behaviour", the entropy index is "a measure of the distribution of commands in the command sample", and the newness index is "a measure of the number of new commands which have not occurred earlier" [5].

GP was employed in this domain only a few years after the approach was first proposed. GP is an evolutionary algorithm with similar operators to GA. Crosbie and Spafford (1995) used GP to evolve autonomous agents for network based intrusion detection. One focus of their paper is on dealing with fitness evaluation and different feature information when evolving the trees [11].

3.1 Swarm Intelligence Techniques

A swarm can be considered as a group of cooperating agents to achieve some purposeful behaviour and task. The simple scheme of a swarm is shown in Figure 3. It links to artificial life, in general, there are several collective behaviour like birds flocking, ant colonies, social insects and swarm theory [37].

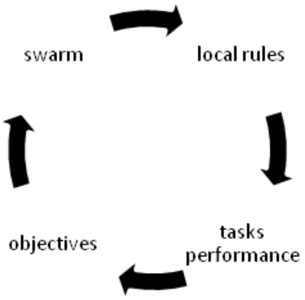

Figure 3. Scheme of a swarm

The term Swarm Intelligence (SI) introduced by Beni and Wang (1989)[8] has received widespread attention in research, mainly as Ant Colony Optimization (ACO), Particle swarm Optimization (PSO) and Bee Colony Optimization (BCO). The foraging behaviour of ants and their ability to find the shortest path from their nests to food source as shown in Figure 4, has inspired the creation of the algorithmic model which is known as Ant Colony Optimization.

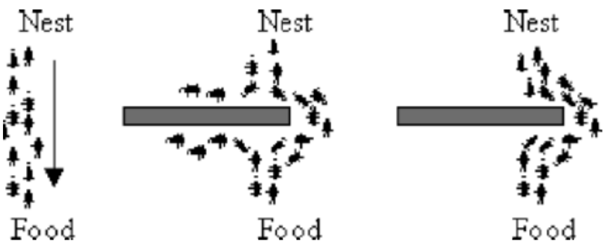

Figure 4. Behaviour of ants

Deneubourg et al. (1990b) [12] presented the double bridge experiment in which nest and food source were separated by a bridge of two branches of equal lengths. Goss et al. (1989) extended the experiment by using paths of unequal lengths in which the majority of the ants choose the shortest path as shown in Figure 5.

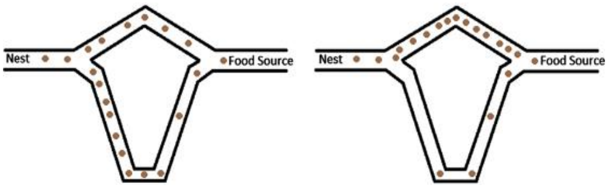

Figure 5. Double Bridge Experiment

Several ACO algorithms have been proposed in the literature and the variants of ACO algorithm [15] is given in Table 4.

Table 4. Variants of ACO

ACO algorithm	Authors
Ant System (AS)	Dorigo (1992); Dorigo et al. (1991a,b, 1996)
Elitist AS	Dorigo (1992); Dorigo et al (1991a,b, 1996)
Ant-Q	Gambardella & Dorigo (1995); Dorigo & Gambardella (1996)
Ant Colony System	Dorigo & Gambardella (1997a,b)
MAX–MIN AS	Stutzle & Hoos (1996, 2000); Stutzle (1999)
Rank-based AS	Bullnheimer et al (1997, 1999c)
ANTS	Maniezzo (1999)
Hyper-cube AS	Blum et al (2001); Blum & Dorigo (2004)

Dorigo et al. (1999, 2004) presented an algorithmic implementation of the ant behaviour for solving minimum cost path problems on graphs known as simple Ant Colony Optimization. ACO is set apart from the other approaches, as it is primarily applied to combinatorial optimisation. There are recent ACO algorithms proposed for continuous numerical optimisation, (Dréo and Siarry (2002) and Socha and Dorigo (2006) [16][33]), however, their application to this domain is limited. ACO represents the problem as a graph and treats it as combinatorial optimisation.

Kennedy and Eberhart (1995) introduced the term Particle Swarm Optimization and their work was the main influence of the basic PSO model. According to this model a fitness function exists which measures the quality of the current solution. A number of particles (solutions) are placed randomly inside the hyperspace, each having a random velocity. The particles move in the hyperspace and at each step evaluates their position according to the fitness function. Each particle in the swarm represents a possible solution. Two key features of this model are: (a) the speed (and therefore the next position) of each particle is calculated according to the findings of both that particle and the findings of the rest of the swarm and (b) the global best solution is communicated among all particles of the swarm. Dozier et al., (2004) presented PSO technique that can be used as a part of IDS to identify possible attacks. The basic variants of PSO have been developed to improve speed of convergence and quality of solution found by the PSO. Recently, there are many variants of PSO and is given in Table 5.

Table 5. Variants of PSO

Particle Swarm Optimization(PSO)	
Basic variants of PSO	**Modified variants of PSO**
• Velocity Clamping • Inertia Weight • Constriction Coefficient • Synchronous and Asynchronous updates	• Single Solution of PSO • Niching with PSO • Constraint Optimization using PSO • Multi-objective Optimization • Dynamic Environment of PSO • Binary PSO • Discrete PSO

3.2 Swarm Intelligence in intrusion detection

In this section, we describe various approaches of swarm intelligence in the field of intrusion detection. Table 6 describes the comparison of various approaches and its performance.

Hai-Hua Gao et al. (2005) proposed a novel intrusion detection approach by applying ant colony optimization for feature selection and SVM for detection**.** The optimal intrusion feature selection was then transformed into the problem of ant traversing through the graph where a certain number of nodes were visited that satisfied the traversal stopping criterion. The fisher discrimination rate (FDR) was adopted as the heuristic information for ant colony optimization, the SVM classifier was adopted as the base classifier to evaluate the feature subset generated by ants' traverse. For experiments, they adopted KDD Cup99 dataset and partitioned the dataset it into three groups: DoS intrusion detection dataset, Probe intrusion detection dataset, U2R&R2L intrusion detection dataset and evaluated ACO-based feature selection method on each dataset respectively. The result showed that using ACO-SVM, Probe dataset achieved the total correct classification rate as 99.4%. Similarly, for Dos dataset, it was 95.2% and for U2R&R2L dataset, it was 98.7%. Also the performance of ACO-SVM was compared with SVM (without feature selection) and the results showed that SVM obtained optimal feature subset and achieved better generalization performance than without feature selection [18].

Soroush et al. (2006) proposed ACO for intrusion detection based on the classification Ant-Miner extracting algorithm (Parpinelli et al., 2002). Ant-Miner itself is inspired by the foraging behaviour of ants in order to classify numerical data to one of some predefined classes. In particular, this algorithm utilizes ants to construct a set of candidate rules of the type: if ($term_1 term_2$…..$term_n$) then $class_c$. In this case $term_i$is formed by (a) an attribute of a record of the dataset, (b) an operator and (c) a value. Quality is measured by taking the confusion matrix of real and predicted instances, i.e. the number of true positives, false positives, false negatives and true negatives with respect to the training set. During the process, the pheromone increases for the terms used for the construction of a rule proportional to the performance of the constructed rule. At the same time it decreases for all other terms (evaporation). Among the discovered rules the best one is selected and augmented to the discovered rules. This is done iteratively until a large base of rules is constructed which can be later on used in test sets as criteria for classifying network connections into intrusive or normal. The experimental results showed that the detection rate of the system increased only by 0.1%. At the same time it reduced the false alarm rate by 1.4% comparing to the original Ant-Miner algorithm [34].

He et al. (2007) proposed the following approach: "*In the problem graph... each node represents a condition that may be selected as part of the crisp rule antecedent being built by an ant. An ant goes round the graph selecting nodes according to a constraint satisfaction method, building its rule antecedent. The rule conclusion is assigned afterwards by a deterministic method*". They take an iterative approach to determine the final rule set. Once one run of the ACO algorithm is completed, the 'best' rule is added to a rule base. The instances in the training set covered by this rule are deleted, and the process is repeated until the number of uncovered instances in the training set is below a predefined threshold. The fitness function used in these population based search/optimisation techniques is very important which considered as detection accuracy [19].

Junbing et al. (2007) proposed an Ant-Miner based classification system. Its main contribution is the introduction of multiple ant colonies instead of a single one that the ant-miner normally employs. The authors noticed that the algorithm might be pushed back in the case where ants searching for best rules of a class B, have been misled by the pheromone trails deposited at a prior time, by ants searching for rules of a class A. In this case, each class is handled by different ant types organized into colonies. That is, each ant that belongs to a colony deposits a distinct type of pheromone which affects only the ants belonging to the same colony. Colonies are searched in parallel to finally discover one rule per colony. The rule with the best quality is selected and added to the rule set. The experimental results showed that the overall system detection rate was increased by 6.02% but false alarm rate was reduced only by 0.08% [21].

Ramachandran et al. (2008) proposed *Fork* which is another IDS based on a variation of the Ant-Miner algorithm. In this case, the algorithm (and the IDS itself) was optimized to function under the constraints of ad-hoc networks. Due to the inherent limitation of these networks in terms of resources it is possible that some nodes may be unable to perform intrusion detection. Therefore, nodes may produce an intrusion detection task request and propagate it to the other nodes. Then the nodes compete according to an auctioning system for performing these tasks. The actual recognition of the intrusive network behaviour is done by the winner nodes. The modifications on Ant-Miner which is responsible for this task include: (a) the priority assignment strategy: a method which identifies candidate solutions that may act as obstacles to the creation of rules and gives them priority. (b) Use of modularity: a method of forming clusters of similar pathways in the solution graph. Thus, terms that belong to the same cluster can be added without being evaluated by the heuristic function. (c) Use of attack thresholds: These modifications improved the processing time for the formation of more accurate rules [32].

Mohamadi H (2008) proposed Simulated Annealing (SA) based fuzzy system to develop an Intrusion Detection System (IDS). The use of SA in IDS is an attempt to effectively explore and exploit the large search space associated with intrusion detection classification problem. Experiments were carried out on 10% of KDD Cup99 dataset of UCI KDD archive. Due to the imbalanced records in the dataset a subset of the dataset was used as training and testing sets (20752 randomly generated samples) and normalized between 0.0 and 1.0. Initial set of fuzzy if-then rules was generated and initial temperature was set as 100. The fitness of the rule was evaluated by number of correctly classified training patterns. The results showed that average accuracy rate obtained was varying from 94% to 99% with the number of rules ranging from 50 to 100. This approach was compared with the different baseline classifiers including pruning C4.5, Naïve Bayes, K-NN, SVM and multi-objective genetic fuzzy IDS. The results showed that the proposed approach obtained highest accuracy (92.89%), better precision, lowest classification cost (0.2093), F-measure, recall than other classifiers [28].

Works of Abadeh et al. (Abadeh et al. 2008; Abadeh and Habibi, 2010) [1][2] and Alipour et al. (2008)[3] were among the first that combined genetic algorithms and ACO for the induction of accurate fuzzy classification rules. Fuzzy set theory has been applied successfully in the past in the field of intrusion detection and has proven to provide very competitive DR and FAR percentages. The combination of Fuzzy set theory, Genetic Algorithms and SI was expected to boost the performance of IDS. An initial population of fuzzy if-then rules was randomly generated. This population was then evaluated and in the process, genetic operations take place so that a new population can be produced by generating new rules. At this point, the ant colony algorithm takes a fuzzy rule and modifies it by performing a number of predefined changes so that an improved version of the same rule was produced. The algorithm then continues as normal by replacing a pre-specified number of if-then rules with newly generated ones and finally stops according to some termination rules. By doing so, the entire (global) search capability of the algorithm was enhanced.

Michailidis et al. (2008) merged the two soft computing techniques to create an improved system for intrusion detection. During the training phase, the PSO was executed recursively to train the network. Specifically, each particle in the PSO corresponds to the synaptic weights of the network. The optimal synaptic weights were fed to ANN, which conducts the main part of the classification with improved efficiency, during the testing phase [27].

Ma et al. (2008a) proposed a combinatorial technique: Binary Particle Swarm Optimization and Support Vector Machine (BPSO-SVM) where dataset features and the crucial SVM parameters were represented by each particle position. The choice of SVM parameters for the classification process and the selection of the optimum features happen simultaneously in one step instead of two. Then the classification process based on SVM was conducted which (given the inputs from the previous step) was much more accurate [26].

Similarly, Wang et al. (2009) used two different flavours of PSO: the Standard Particle Swarm optimization (SPSO) and Binary Particle Swarm Optimization (BPSO) for seeking optimal SVM parameters and extracting a feature subset respectively. Each particle represents a solution that indicates which features and parameter values should be kept. Finally, the results (selected features and parameter values) along with the training dataset were fed to the SVM classifier which executes normally to classify specific network behaviour as

Table 6. Performance Comparison of various SI methods

SI Techniques/Methods		Author	Year	Normal	Probe	DoS	U2R	R2L	DR	FAR
PSO	PSO-SVM, BPSO,SPSO	Wang et al.	2009	N/A	N/A	N/A	N/A	N/A	99.84	N/A
	BPSO-SVM	Ma et al.	2008	N/A	N/A	N/A	N/A	N/A	96.77	8.01
	QPSO,MQPSO	Liu et al.	2010	N/A	86.48	88.48	N/A	N/A	N/A	N/A
	PSO-SVM	Wang Hui et al.	2011	N/A	N/A	N/A	N/A	N/A	95.635	N/A
	GQPSO-SVM	Shangfu Gong	2011	N/A	91.77	99.98	100	98.26	N/A	N/A
ACO	GA-ACO	Alipour et al.	2008	98.5	82.5	98.5	76.3	89	95.5	0.0018
	GA-ACO	Abadeh Habibi	2010	96	86.25	98.83	72.8	33.45	94.33	N/A
	ACO-SVM	Hai-Hua Gao et al.	2005	N/A	99.4	95.2	98.7		N/A	N/A
	Multiple ant colony	Junbing et al.	2007	99.9	N/A	N/A	N/A	N/A	98.42	0.14
	Modified ant-miner	Soroush et al.	2006	N/A	N/A	N/A	N/A	N/A	Increased by 0.1%	Reduced by 1.4%
	DPE1-ant miner	Soroush et al.	2005	N/A	N/A	N/A	N/A	N/A	99.5	2.7
	DPE2-ant miner								99.1	2.1
	Hybrid EFS	Mohammed Saniee Abadeh et al.	2007	N/A	N/A	N/A	N/A	N/A	99.5	0.001831

intrusive or normal [36]. Liu et al., (2009) applied two variations of PSO, namely Quantum Particle Swarm Optimization (QPSO) and Modified Quantum Particle Swarm Optimization (MQPSO) for intrusion detection system.

Chang-Lung et al. (2009) described an intrusive analysis model based on the design of honeypots and ant colony. In this model, all network assets of the honeypot were associated with a pheromone value. After intrusions or other malicious behaviour the honeypot was configured in a way so that the amount of pheromone of each affected asset was increased. Next, the ACO was applied to trace the trail of attack and analyze the habits and interests of aggressors. Muraleedharan and Osadciw (2009) adopted a similar approach by integrating honeypot architecture and the ACO algorithm in the sensor network. In this case, a number of inexpensive nodes were actually used as a part of the IDS while it appears as a normal part of the sensor network. Tracking intruders was done in a similar way [10].

Oliveira R.L et al. (2009) performed a comparative analysis of three bio-inspired meta-heuristics: Fuzzy Genetic System (FGS), fuzzy artificial immune system and ant colony optimizer to perform data mining classification task. They also presented a methodology that integrated data mining tasks with artificial immune system (AIS) and fuzzy logic called IFRAIS (Induction of Fuzzy Rules with artificial immune System). The feature selection and classification was performed by fuzzy genetic system and Takagi-Sugeno-Kang (TSK) fuzzy rules were generated automatically from the datasets and GA was applied to find the shortest and most accurate subset of rules. For experimentation, six datasets from UCI repository were used. The three bio-inspired meat-heuristics were compared with the two well-known algorithms, C4.5 and CN2 in terms of classification accuracy and rule sets. The results showed that FGS obtained higher accuracy in five of the six datasets. The average number of discovered rules was used to verify the simplicity of the discovered rule set which was computed over 10-fold cross validation. It was observed that IFRAIS presented the smaller number of rules in three of the datasets, while Ant-miner was very competitive when concerning number of terms.

Tie-Jun Zhou et al. (2009) proposed an ID Based on Particle Swarm Optimization (PSO) and Support Vector Machine (SVM). The use of PSO-SVM in Intrusion Detection established a classification model; at the same time verified the validity of the model. The size of the fitness can be obtained from the accuracy rate of SVM, the higher accuracy rate, then greater the fitness. Personal best value ($pbest_{id}$) of each particle was set to the current position, using the fitness function, calculated the fitness of each particle, and taking the $gbest_{id}$ of best fitness value as the first global best value ($gbest_{id}$). Comparing the fitness of each particle with its fitness value, if the value was better, updated the $pbest_{id}$, or retained the original value; Comparing the updated each particle $pbest_{id}$ with the global best value, if the value was better, updated the $gbest_{id}$, or retained the original value. Experiments were carried out using KDD Cup99 dataset. They compared the performances of improving PSO-SVM algorithm, PSO-SVM algorithm and SVM algorithm in intrusion detection. The result showed that the proposed improved PSO-SVM algorithm performed better (where recognition rate was 97.2612%, recognition time was 7.98400 / sec and the normal data on the number of support vector were 189) compared to the other algorithms [30]. Arif Jamal Malik et al. (2011) proposed hybrid classifier based on Binary Particle Swarm Optimization (BPSO) and Random Forests (RF) algorithm for the classification of PROBE attacks in a network. In this approach, PSO was used for feature selection and RF for classification. Detection rate was considered as the fitness value of the classifier and the particle with the highest detection rate was considered as the best particle. During the evolution process, the swarm takes the new position in the search space. Again the process of attribute selection and classification were performed. The process stopped when the stopping condition was met. The dataset used for experimentation was KDD Cup99 dataset. A sample of the records was selected by random selection and used five attribute selection techniques. The results showed that average detection rate and false positive rate of PSO-RF was better than all the other classifiers [4].

4. CONCLUSION

The last decade has seen an increasing use of nature inspired computing techniques in engineering applications. Researchers in computer science have developed swarm-based systems in response to the observed success and efficiency of swarms in nature to solve difficult problems. Successful applications of swarm intelligence include the modelling of agent behaviour and various optimization problems such as the routing of packages through networks, the travelling salesman problem scheduling, robotics, network security and data mining. In this paper, various swarm intelligence techniques used by the researchers in evaluating the performance of intrusion detection model was reviewed. From the empirical study performed, this work identified that its application to the intrusion detection domain is limited which is still to be explored.

5. REFERENCES

[1] Abadeh MS, Habibi J. 2010. A hybridization of evolutionary fuzzy systems and ant colony optimization for intrusion detection. The ISC International Journal of Information Security, vol.2, no.1, 33-46.

[2] Abadeh MS, Habibi J, Soroush E. 2008. Induction of fuzzy classification systems via evolutionary ACO-based Algorithms. International Journal of Simulation, Systems, Science, Technology, vol.9, no.3.

[3] Alipour H, Khosrowshahi E, Esmaeili M, Nourhossein M. 2008. ACOFCR: applying ACO-based algorithms to induct FCR. In Proceedings of the World Congress on Engineering (IWCE), 12-17.

[4] Arif Jamal Malik, Waseem Shahzad, Farrukh Aslam Khan. 2011. Binary PSO and Random Forests Algorithms for PROBE attacks Detection in a network. In Proceedings of IEEE Congress on Evolutionary Computation, 662-668.

[5] Balajinath B., Raghavan S.V. 2001. Intrusion Detection through Learning Behaviour Model. International Journal of Computer Communications, vol.24,1202–1212

[6] Banks A, Vincent J, Anyakoha C. 2008. A review of Particle Swarm Optimization, Part II: Hybridisation, Combinatorial, Multi-criteria and Constrained Optimization, and Indicative Applications, Natural Computing, vol.7, 109–124.

[7] Banks A,Vincent J, Anyakoha C. 2008. A review of Particle Swarm Optimization, Part I: Background and Development, Natural Computing, vol.6, 467–484.

[8] Beni, G., Wang, J. 1989. Swarm Intelligence in Cellular Robotic Systems. In Proceedings of NATO Advanced Workshop on Robots and Biological Systems, Tuscany, Italy.

[9] Bing Shuang, Jiapin Chen, Zhenbo Li. 2011. Study on Hybrid PS-ACO algorithm, Applied Intelligence, Springer, vol.34, 64-73.

[10] Chang-Lung T, Chun-Chi T, Chin-Chuan H. 2009. Intrusive behavior analysis based on honey pot tracking and ant algorithm analysis, In Proceedings of the 43rd Annual International Carnahan Conference on Security Technology, 248-252.

[11] Crosbie M., Spafford E.H. 1995. Applying Genetic Programming to Intrusion Detection, In working Notes for the AAAI Symposium on Genetic Programming, 1-8, MIT.

[12] Deneubourg, Aron, Goss, Pasteels. 1990. The self-organizing exploratory pattern of the Argentine ant, Journal of Insect Behavior, vol. 3, no.1, 159 - 168.

[13] Dorigo M, Di Caro G. 1999. The ant colony optimization meta-heuristic, New ideas in Optimization, 11-32.

[14] Dorigo M, Di Caro G, Gambardella L.M. 1999. Ant Algorithms for Discrete Optimization, Artificial Life, vol.5, 137 –172.

[15] Dorigo M, Stutzle T. 2004. Ant colony optimization, MIT Press.

[16] Dréo, J., Siarry, P. 2002. A new ant colony algorithm using the heterarchical concept aimed at optimization of multiminima continuous functions. Lecture Notes in Computer Science, vol.1, 216–227.

[17] Goldberg D. E. 1989. Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley Publishing Co., Massachusetts.

[18] Hai-HuaGao, Hui-Hua Yang, Xing-Yu Wang. 2005. Ant Colony Optimization Based Network Intrusion Feature Selection and Detection. In Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, 3871-3875.

[19] He J, Long D, Chen C. 2007. An Improved Ant-based Classifier for Intrusion Detection. In Proceedings of the Third International Conference on Natural Computation, 819–823.

[20] Holland J.H. 1992. Adaptation in Natural and Artificial Systems: an introductory analysis with applications to biology, control and artificial intelligence. The MIT Press, 2nd edition

[21] Junbing H, Dongyang L, Chuan C. 2007. An improved ant-based classifier for intrusion detection. In Proceedings of the Third International Conference on Natural Computation, 819-823.

[22] KDD99, KDDCup 1999 data. 1999. http://kdd.ics.uci.edu/ Databases/kddcup99/10 percent.gz.

[23] Kennedy J, Eberhart R 1995. Particle Swarm Optimization. In Proceedings of IEEE International Conference on Neural Networks, 1942-1948.

[24] Koza 1992. Genetic Programming: On the Programming of Computers by Means of Natural Selection. MIT Press.

[25] Koza 1994. Genetic Programming 2: automatic discovery of reusable programs. Complex adaptive systems, MIT Press

[26] Ma J, Liu X, Liu S. 2008a. A new intrusion detection method based on BPSO-SVM. In Proceedings of the International symposium on Computational Intelligence and Design, 473-477.

[27] Michailidis E, Katsikas S K, Georgopoulos E. 2008. Intrusion detection using evolutionary neural networks .In Proceedings of the Panhellenic conference on informatics, 8-12.

[28] Mohamadi H, Habibi J, Saniee Abadeh M. 2008. Misuse intrusion detection using a Fuzzy-Meta-heuristic approach. In Proceedings of 2nd Asia Intl. Conference on modeling and simulation, 439-444.

[29] Muraleedharan R, Osadciw L.A. 2009. An intrusion detection framework for sensor networks using honeypot and Swarm Intelligence. In Proceedings of the 6th Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, 1-2.

[30] Oliveira R.L, De Lima B.S.L.P, Ebecker N.F.F. 2007. A Comparison of bio-inspired meta-heuristic approaches in classification tasks. WIT Transactions on Information and Communication technologies, vol.38, 25-32.

[31] Parpinelli RS, Lopes HS, Freitas AA. 2002. Data mining with an ant colony optimization algorithm. IEEE Transactions on Evolutionary Computation, vol.6, no.4, 21-32

[32] Ramachandran C, Misra S, Obaidat MS.2008. FORK: A novel two pronged strategy for an agent-based intrusion detection scheme in ad-hoc network. Computer Communications, vol.31, no.16, 3855-69.

[33] Socha, Dorigo M. 2006. Ant colony optimization for continuous domains. European Journal of Operational Research, vol.185, 1155–1173.

[34] Soroush E, Saniee Abadeh M, Habibi JA. 2006. Boosting ant-colony optimization algorithm for computer intrusion detection. In Proceedings of the IEEE 20th International Symposium on Frontiers in Networking with Applications.

[35] Tie-Jun Zhou, Yang Li, Jia Li. 2009. Research on Intrusion Detection of SVM Based on PSO. In Proceedings of Eighth International Conference on Machine Learning and Cybernetics, 1205-1209.

[36] Wang J, Hong X, Ren R, Li T. 2009. A real-time intrusion detection system based on PSO-SVM. In Proceedings of the International Workshop on Information Security and Application, 319-321.

[37] C. Grosan et al.: Swarm Intelligence in Data Mining, Studies in Computational Intelligence (SCI) 34, 1–20 (2006),_Springer-Verlag.

[38] Shelly Xiaonan Wu, Wolfgang Banzhaf. 2010. The use of computational intelligence in intrusion detection systems: A review", Applied Soft Computing, pp.1-35, Elsevier Publication

[39] Stutzle, T., & Hoos, H. H. 1996. Improving the Ant System: A detailed report on the MAX-MIN Ant System. Technical report AIDA-96-12, FG Intellektik, FB Informatik, TU Darmstadt, Germany.

[40] Stutzle, T., & Hoos, H. H. 2000. MAX-MIN Ant System. Future Generation Computer Systems, 16(8), 889–914.

[41] Stutzle, T. 1999. Local Search Algorithms for Combinatorial Problems: Analysis, Improvements, and New Applications, vol. 220 of DISKI. Sankt Augustin, Germany, Infix.

[42] Maniezzo, V. 1999. Exact and approximate nondeterministic tree-search procedures for the quadratic assignment problem. INFORMS Journal on Computing, 11(4), 358–369.

[43] Dorigo, M. 1992. Optimization, Learning and Natural Algorithms. PhD thesis, Dipartimento di Elettronica, Politecnico di Milano , Milan.

[44] Dorigo, M., Maniezzo, V., & Colorni, A. 1991a. Positive feedback as a search strategy. Technical report 91-016, Dipartimento di Elettronica, Politecnico di Milano, Milan.

[45] Dorigo, M., Maniezzo, V., & Colorni, A. 1991b. The Ant System: An autocatalytic optimizing process. Technical report 91-016 revised, Dipartimento di Elettronica, Politecnico di Milano, Milan.

[46] Dorigo, M., Maniezzo, V., & Colorni, A. 1996. Ant System: Optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man, and Cybernetics—Part B, 26(1), 29–41.

[47] Dorigo, M., & Gambardella, L. M. 1996. A study of some properties of Ant-Q. In H. Voigt, W. Ebeling, I. Rechenberg, & H. Schwefel (Eds.), Proceedings of PPSN-IV, Fourth International Conference on Parallel Problem Solving from Nature, vol. 1141 of Lecture Notes in Computer Science (pp. 656–665). Berlin, Springer-Verlag.

[48] Gambardella, L. M., & Dorigo, M. 1995. Ant-Q: A reinforcement learning approach to the traveling salesman problem. In A. Prieditis & S. Russell (Eds.), Proceedings of the Twelfth International Conference on Machine Learning (ML-95) (pp. 252–260). Palo Alto, CA, Morgan Kaufmann.

[49] Dorigo, M., & Gambardella, L. M. 1997a. Ant colonies for the traveling salesman problem. BioSystems, 43(2), 73–81.

[50] Dorigo, M., & Gambardella, L. M. 1997b. Ant Colony System: A cooperative learning approach to the traveling salesman problem. IEEE Transactions on Evolutionary Computation, 1(1), 53–66.

[51] Bullnheimer, B., Hartl, R. F., & Strauss, C. 1997. A new rank based version of the Ant System—A computational study. Technical report, Institute of Management Science, University of Vienna, Austria.

[52] Bullnheimer, B., Hartl, R. F., Strauss, C. 1999c. A new rank-based version of the Ant System: computational study. Central European Journal for Operations Research and Economics, 7(1), 25–38.

[53] Blum, C., & Dorigo, M. 2004. The hyper-cube framework for ant colony optimization. IEEE Transactions on Systems, Man, and Cybernetics – Part B

[54] Blum, C., Roli, A., & Dorigo, M. 2001. HC–ACO: The hyper-cube framework for Ant Colony Optimization.In Proceedings of MIC'2001—Metaheuristics International Conference, vol. 2 (pp. 399–403).

[55] Wang J, Hong X, Ren R, Li T. 2009. A real-time intrusion detection system based on PSO-SVM. In: Proceedings of the International Workshop on Information Security and Application. pp. 319-321.