ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

A Survey on Intrusion Detection Techniques

Dr.V.Praveena[1], M.Showmyaa[2], B.Sathya[3]

Assistant Professor, Department of CSE, SNS College of Technology, Coimbatore, India[1]

U.G. Student, Department of CSE, SNS College of Technology, Coimbatore, India[2, 3]

ABSTRACT: Communication through network should be more reliable and secured. One of the most important detection methods was intrusion detection system. An intrusion detection system (IDS) is device or software application that monitors a network or system for malicious activity or policy violations. In order to avoid the false alarms and increase the performance we go for some techniques. They are Ant Colony Optimization Algorithm (ACO), Bees Colony Optimization Algorithm (BCO), and Particle Swarm Optimization Algorithm (PSO). In this paper a survey is made on the various Intrusion Detection Techniques namely Ant colony Optimization Algorithm (ACO), Bee Colony Optimization Algorithm (BCO), and Particle Swarm Optimization Algorithm (PSO).

KEYWORDS: Communication, Intrusion, Optimization, Security, Detection.

I. INTRODUCTION

Wireless Sensor Network (WSN's) is vulnerable to various sorts of security threats due to the following reasons: Scalable, scattered, dynamic, fault, tolerant and weak infrastructure in nature. So, this network's can easily be targeted to various security threats. Network security infrastructure depends upon intrusion detection system. Intrusion detection System that provides security from unknown intrusion attacks. Traditional security policies or firewalls have difficulty in preventing such as an additional wall for protecting systems despite the prevention techniques.

IDS can be a great tool for monitoring and protecting the network from malicious activity, however, they are also prone to false alarms. The need of IDS to be properly configured to recognize what is normal traffic on your network, what might be malicious traffic, or the administrators responsible for responding to IDS alerts, the alerts need to be analysed and respond effectively.

The main objective of this paper to study about existing algorithms and comparisons of them on basis of advantages, disadvantages and feature, etc…Monitoring, detecting and responding to unauthorized activity by company insiders and outsider intrusion are the three essential functions served by IDS. IDS use the policies to define certain events that, if detected will issue an alert. In other words, an alert will be issued and detected if a particular event is considered to constitute a security incident. In some IDS, the administrator will receive a notification of a possible security incident in a form of email, page, or SNMP trap for sending out alerts. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event.

In this section we describe the algorithms such as Ant Colony Optimization Algorithm [2], Bees Colony Optimization Algorithm [3], and Particle Swarm Optimization Algorithm [5].

II. RELATED WORK

In [1] this paper, they have proposed the IDS model uses the feed forward and the back propagation algorithms along with various other optimization techniques to minimize overall computational. In [2] this work, they first gave a detailed description of the origins and the basics of ACO algorithms and presented the hybridization with beam search and with constraint programming. The main idea behind these two approaches is the reduction of the search space that has to be explored by ACO. This can be especially useful when large scale problem instances are considered.

In [3] have presented the quantum inspired bee colony optimization. The proposed method can simultaneously adjust two parameters of a qubit and automatically achieve the best match between two adjacent quantities, which may

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

accelerate the optimization process. In [4] this work, ABC algorithm is used for optimizing the multivariable function and results produced by ABC, GA, GSO and PSEA have been compared.

In [5] this paper proposes a technique for intrusion detection using Particle Swarm Optimization with Genetic Algorithm based feature selection and using Adaptive Mutation for slow convergence of optimization algorithm. The results thus obtained are approximately 92% that proves the proposed approach to be quite effective in intrusion detection.

In [6] research work, they have proposed a new approach called outlier detection where, the anomaly dataset is measured by the Neighbourhood Outlier Factor (NOF). Here, trained model consist of big datasets with distributed storage environment for improving the performance of Intrusion Detection System. In [7] have presented on improved artificial bees colony (iABC) algorithm iABC is based on neighbour selection mechanism for onlooker bees. It is mentioned that the control parameter of iABC (k constant) should be adjusted depending on the structure of optimization problem.

In [8], the swarm-intelligence-based intrusion detection system model proposed in this paper better solves the problems by means of decomposing of detection functions, corresponding separation of data. In [9] this paper, they develop a novel metric to assess the performance of Intrusion Detection System under the influence of attacks they proposed a new metric called feedback reliability ration of an Intrusion Detection System.

In [10] this paper, a similar approach can be used find near-optimal solution to the travelling salesman problem. The food source is depleted, and hence the route is no longer populated with pheromones and slowly decays. Because the ant-colony works on a very dynamic system, this algorithm works very well in graphs with changing topologies. Computer networks and artificial intelligence simulations of workers are the examples.

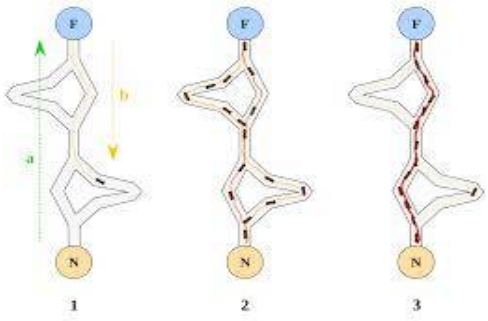
In [11] this paper, the study of how best to apply ACO to such variations will certainly be one of the major research directions in the near future. ACO algorithm is another research direction that will be pursued in the future.

In [14] this paper, the intrusion detection is to automatically scan network activity and detection attacks In [15] this paper, they have discussed and analysed the impact factor of intrusion behaviours. With the ability of strong self-learning and faster convergence, this intrusion detection method can detect various intrusion behaviours rapidly and effectively by learning the typical intrusion characteristic information. Using rough set to reduce dimension and they have applied this technique on KDD99 data set and get satisfactory results. The experimental result shows that this intrusion detection method is feasible and effective.

III. TECHNIQUES OF IDS

A. Ant Colony Optimization (ACO)

Ant colony optimization tries to improve the rate of better detection. Ant colony optimization is a probability technique for solving computational problems which can be reduced to finding good paths through graphs based on the strategies for real ants [12]. In ant colony optimization algorithm, each artificial ant is considered as a simple agent, communicating with other ants only indirectly and by effecting changes to a common environment.



ACO to detect the network risks

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

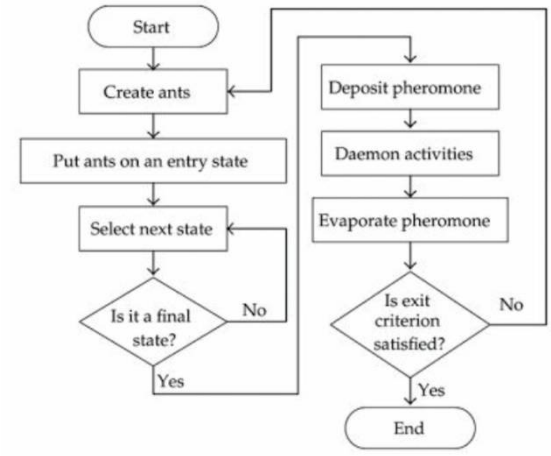
The first algorithm was aiming to search for an optimal path in a graph, based on the path of ant's behaviour between their colony and a source of food [10]. The original idea has since diversified to solve a wider class of numerical problem and as a result, several problems have emerged, drawing on various agents of the behaviour of ants [11]. The main feature is high precision solution, fast search speed convergence to global optimum and greedy heuristic search. The improved versions of ACO is

- ACS
- MAX-MIN
- AS
- AS rank

In real concepts, ants wander randomly, and after getting food return to their colony while laying down trails. If other ants find such a path, then this path is likely to follow the trail, not randomly. When those ants find food the trail starts evaporating then this will affect the strength of the trail. The advantage of the pheromone evaporation is avoiding the convergence to a locally optimal solution [12]. In times of no evaporation, the paths chosen by the first ants would tend to be excessively attractive to the following ones. In that case, the exploration of the solution space would be constrained. When one ant find a good path (i.e., short) from the colony to a food source. Thus, other ants are more likely to follow that path.

Pseudo code for Ant Colony Optimization:

1: Initializing pheromone trail
2: while criteria stops not met do
3: For all ants do
4: Randomly traces path
5: while get incomplete solution do
6: Next select element randomly according to pheromone trail
7: end while
8: end for
9: Update pheromone trail
10: end while



Flowchart for ACO

ACO is the foraging behavior of real ants. The sequence of decisions is not independent (i.e. random). Hence theoretical analysis is difficult and the research is independent. Thus, the above ideas show that the ACO is not more effective and also results in convergence.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

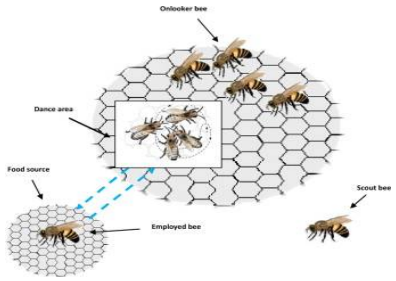
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

B. Bees Colony Optimization (BCO)

The Bees Algorithm is a population based search algorithm, it mimics the food foraging behaviour of honey bee colonies [3]. In this concept, the algorithm performs a kind of neighbourhood search combined can be used for combitorial optimization and continuous optimization. The only condition for the application of bees is that some measure of topological distance between solutions is defined.



A typical bee colony model

Many researches such as [4] and [7] have argued that social insects behaviour system provides us with a powerful metaphor that can be applied on IDS problems. The critical maintenance of the integrity of the social insect colonies is to analyze and detect the intrusion. In this approach, we stick on the honeybee in nature, which faces the analogous security problems. Honeybees survive in difficult environments with different levels of threats to security. Those threats motivate the bees to detect and respond quickly on any aggressive acts when someone attacks the colony.

The problem faced by the honeybee guard is the same as the one faced by IDS, which is to distinguish between the intruder and the nest-mate. Honeybee colony has a small entrance which is patrolled by its workers called guards who allow nest-mates and deter the intruders. The entrance guards intercept and examine incomers at the nest-entrance and differentiate between nest mates and non-nest mates [4]. The two methods Undesirable-Absent (UA) and Desirable-Present (DP) that the honeybee guard uses in filtering the incomer are applied to the IDS.

The Bees algorithm is an optimization algorithm inspired by the natural foraging behavior of the honeybee to find the optimization algorithm [7]. The required set of number of parameters like n-he number of scout, e-the number of best sites out of m selected sites, n-the number of sites selected out of v visited sites, (n-m)-number of bees recruited for the other selected sites.

Pseudo code for Bees Colony Optimization:

1. Initialize population with random solutions.
2. Evaluate fitness of the population.
3. While stopping criterion not met forming new population.
4. Select sites for neighborhood search.
5. Recruit bees for selected sites (more bees for best e sites) and evaluate fitness's.
6. Choose the fittest bee from each patch.
7. Assign the remaining bees to search randomly and evaluate their fitness's.
8. End while.

One of the important requirements of the technique is the ability of learning. Moreover, this technique is supposed to distinguish between different characteristics after some level of training. The main component of the model is the neural network. Ability of learning, generalizing attributes even with noisy data, and the capability of classifying patterns effectively are the features of neural network. These features can be further used to improve the detection and reduce false alerts in the IDS.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

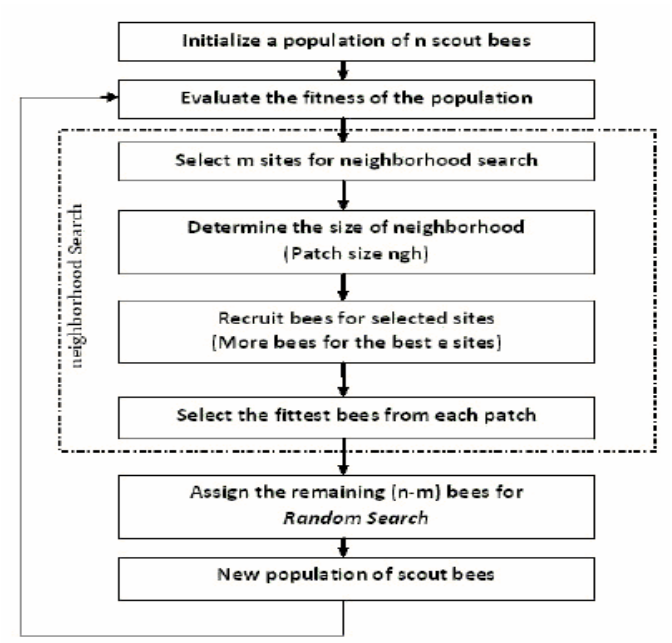
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Neural Network are not used in BSO because it has some drawbacks such as a computational complexity, slow of learning process, and difficulty of parameter settings [3]. These problems will result to the poor performance of the detection of the system.



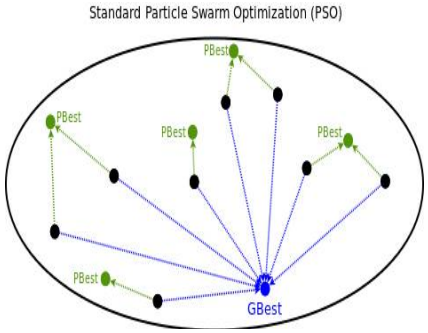
Flowchart for BSO

As Neural Network are not used in BCO has an advantage over it. Therefore, many global optimization techniques have been proposed to train the neural network to tackle these problems and enhance the learning efficiency such as Particle Swarm Optimization.

C. Particle Swarm Optimization (PSO)

By inspiration from animal's collective behavior such as animal flocking, fish spooling and ant colonies, artificial intelligence researchers proposed optimization techniques called swarm intelligence (SI).

Swarm intelligence is a distributed solution to complex problems which intend to solve complicated problems by interactions between simple agents and their environment. Particle swarm optimization has several advantages compare with the other algorithms in this group such as simple to implement, scalability, robustness, quick in finding approximately optimal solution and flexibility.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

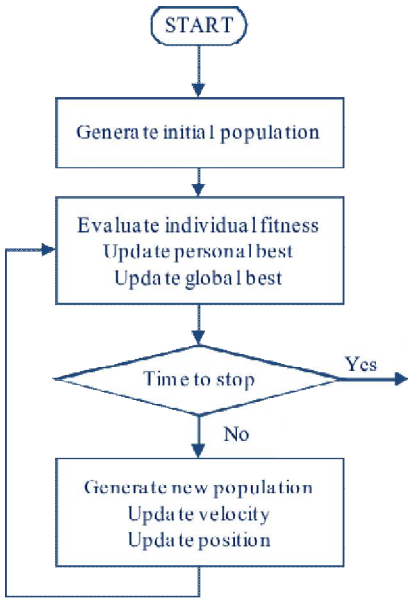
Vol. 5, Issue 9, September 2017

Each particle keeps track of best value achieved so far by it called pbest and the best value of neighboring co-ordinates called gbest as well. Particle keeps on changing their flying velocity (acceleration) based on pbest and gbest locations leading to optimal solution.

Pseudo code for Particle Swarm Optimization:

```
For each particle
   Initialize particle
END
Do
For each particle
  Calculate fitness value
     If the fitness value is better than the best fitness value (pBest) in history
        Set current value as the new pBest
End
Select the particle with the best fitness value of all the particles as the gBest
   For each particle
      Calculate particle velocity
      Update particle position
End
```

Each individual is called particle in PSO. In standard PSO, after the initialization of the population, each particle update its velocity and its position in each iteration based on their own experience and the best experience of all particles. At the end of each iteration the performance of all particles will be evaluated by predefined cost functions.



Flowchart for PSO

This is nature inspired technique based on social behavior of birds flying in the sky in search of goal i.e., food, etc.., or fish behavior to get protection from giant fishes. While flying, birds adjust their flying as per heir flying behavior of itself as well as other members of the flock. Each of the members tries to reach optimum position

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

PSO has a very few parameters to adjust and has proved to be an effective technique on routing techniques. Each particle tries to modify its position using the following information:

- Based on the current positions,
- Based on the current directions,
- Based on the distance between the current position and the pbest,
- Based on the distance between the current position and the gbest.

In a standard PSO algorithm, each dimension of a particle can only be set as real values. In discrete optimization problems such as feature selection of network connection records in DARPA data, it was somewhat hard to use. Data sets with unimportant, noisy or highly correlated features will significantly decrease the classification accuracy rate. By removing these features, the efficiency and classification accuracy rate can be obtained.

IV. CONCLUSION AND FUTURE WORK

In recent years, many researchers have been done to develop an effective mechanism for IDS. An effective IDS is defined when it can simultaneously obtain both high classification accuracy and low false alarm rates. In this paper, we have provided the comparative study of some intrusion detection system approaches like Bee Colony Optimization Algorithm (BCO), Ant Colony Optimization Algorithm (ACO), and Particle Optimization Algorithm (PCO). Each Algorithm try to do best in a particular way but there are always some limitations. From this survey paper, we conclude that in several research areas using PCO are faster, efficient and cheaper when compared with other techniques,

REFERENCES

1. Basant Subha, Santosh Bisuas, Sushanta Karmakar,"**A Neural Network Based System for Intrusion Detection and Attack",** doi: 10.1109/NCC.2016.7561088.
2. Christian Blum,"**Ant Colony Option: Introduction and Recent Trends"**, physics of life reviews 2(2005)353-373.
3. D.Karabog, **"An Idea Based on Honey Bee Swarm for Numerical Optimization"**, TR-06, October-2005.
4. D.Karaboga, B.Basturk "**A Powerful and Efficient Algorithm for Numerical Function Optimization: Artificial Bee Colony (ABC) algorithm"**, J Glob option (2007)39:459-471.
5. Dattatray V. Jadhav, Bharat Rathi, **"Network Intrusion Detection Using PSO Based on Adaptive Mutation and Genetic Algorithm",** International Journal of Scientific & Engineering Research, Volume 5, Issue 8,August-2014 ISSN 2229-5518
6. J.Jabeza, B.Muthu kumar,"**Intrusion Detection System"**, International Conference on Computer Communication and Convergence (ICCC 2015).
7. Kiran.M and Babalik.A (2014), **"Improved Artificial Bee Colony Algorithm for Continuous Optimization Problems"**, Journal of Computer and Communications 2,108-116. doi:10.4236/jce.2014.24015.
8. Lianying Z, Fengyu L,"**A Swarm-Intelligence-based Intrusion Detection Technique",** +IJCSNS International Journal of Computer Science and Network Security 2006: 6(7):146-50.
9. Lippmann R, Haines JW, Fried JD, Korba J, Das K. "**The 1999 DARPA off-line Intrusion Detection, Evaluation Computer Networks"**,2000;34(4):579-95.
10. Macura Wiktor.K, **"Ant Colony Algorithm"**, from Math World-A Wolfram web resources, created by Eric.W Weistein.
11. Marco Dorigo, Mauro Birattari, Thomas Stuzle, **"Ant Colony Optimization"**, IEEE Computational Intelligence Magazine (volume 1, Issue 4, Nov 2006).
12. Nada M.A.Ac-Salami, saad Ghaleb Yaseen, **"Ant Colony Optimization"**, IJCSNS International Journal of computer science and Network security, VOL8 no.6,pp 351-357,june 2008.
13. Nilotpal Chakraborty, "**Intrusion Detection System and Intrusion Prevention System: A Comparative Study"**, International Journal of Computing and Bussiness Research (IJCBR) ISSN (online):2229-6166
14. Srinoy S, **"An Adaptive IDS model based on Swarm Intelligence and Support Vector Machine"**, In: Proceedings of the International Symposium on Communications and Information Technologies 2006. p. 584-589.
15. Tian W, Liu J, "Intrusion **Detection Quantitative Analysis with Support Vector Regression and Particle Swarm Optimization Algorithm**", In: Proceedings of International Conference on the Wireless Networks and Information Systems, 2009 (WNIS '09).p. 133-136.