SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Vol. 1 Isuue 1

# A Survey on Application of Swarm Intelligence in Network Security

**Muhammad Saad Iftikhar[1], Muhammad Raza Fraz[2]**

*[1, 2] School of Electrical Engineering and Computer Science- SEECS*

*National University of Science and Technology- NUST, Pakistan*

*[1]m.saad.iftikhar@gmail.com , [2]raza_fraz@hotmail.com*

## ABSTRACT

Nowadays security is an essential part of every framework. In past few years due to the increase in access of malicious data over the Internet resources the security becomes a necessary component. Swarm intelligence is an emerging and new biological field of optimization. The researchers have already developed many algorithms by studying the behavior of different swarms of incest such as Ants Bees etc. After the success of swarm intelligence in other areas researchers now started work in the field of security too. In this survey paper we tried to find out the reason of network security and how swarm intelligence method have been used to make system efficient in term of performance by providing network security..

**Keywords:** Network Security, Swarm Intelligence, Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), Ant Colony Clustering (ACC), Survey

# 1. INTRODUCTION

The use of computer and Internet is increasing day by day and they both can bring significant changes in the quality of life style of many people. In the last few years, different techniques were proposed and successfully deployed to secure the computer systems from unauthorized use. Such techniques include additional software and hardware systems like anti-virus software, firewall, secured network protocols, password protection, message encryption,

M.S. Iftikhar and M. R. Fraz; *A Survey on Application of Swarm Intelligence in Network Security* in Transactions on Machine Learning and Artificial Intelligence, Volume 1, No 1 (2013), PP 01-15
*URL: http://scholarpublishing.org/index.php/TMLAI/article/view/24/TMLAI-13-1005*
*Publication Date: December 17th 2013*

and many other security tools. With the passage of time the security methods are enhanced and hence so the methods used by attackers.

Many of the already existing networks and the new emerging technologies are expected to be secure from such Trojans and virus attacks. Systems like Mobile Ad-Hoc Networks (MANET) [1] and Wireless Sensor Networks (WSN) [2] have their own security deficiencies and vulnerabilities. It is almost impossible to make system completely secured regardless of the intrusion detection or prevention techniques. Since the already invented approaches failed to fully secure the systems the need of the new protection system or technique is essential for this purpose the intrusion detection becomes the most important part of every network for the security purposes as a second line defense after the firewalls.

In security system intrusion detection systems plays an important role in attack detection, and network inspection to protect the network or computer from any malicious data or to identify these threats. Thus such system must be efficient with respect to detection rate. After the appearance of first intrusion detection system numbers of techniques have been introduced to provide security and enhance the network performance. Few such approaches are Statistical approach, Rule Base approach, Expert System approach, Hybrid approach and Pattern Recognition technique.

Now in recent years researchers have developed interests in the field of biology and natural systems [3]. Swarm Intelligence as one of the innovative distributed paradigm that studies the behavior of swarms of insects and animals for solving complex optimization problem. Behaviors such as finding paths to food sources, organizing their nests, moving from one place to any other place in an organized way are analyzed and modeled. The security systems in networks had applied these models for the intrusion detection purpose. The purpose is to perform some significant measures such as tracing the attack source, distinguish between a normal and abnormal behavior.

Researchers are being motivated because these natural systems have many characteristics that might be used for the security purposes. Like, a swarm of insect with very confined capabilities still finishes very complex tasks. Swarm based security systems or intrusion detection systems are light in weight and simple to put into practice. They are quite robust, vastly adaptive to different conditions and more importantly self-configurable. The biology immunity mechanism has given us much reference particularly to network security. Such as intrusion detection systems, that is based on artificial immunity. The main advantage of approaching security through swarm intelligence is due to the increasing interests of swarm intelligence in the academic and industry fields. In this paper we tried to categorize the work that has been done in the field of swarm intelligence based security networks.

# 2. RELATED TERMS

## 2.1 Network Security

Network security is a generalized term used in computer networks in order to secure them from threats viruses Trojans and all the attacks that can cause damage to the computer network infrastructure. It is typically managed by some administrator a system or network administrator who can protect the whole network as well as all the recourses associated with it by implementing some security tools, software and hardware.

In computer world the word security refers to the ability of the system to protect and manage sensitive data. For example when data transmission is going between two nodes A and B over link X no one should be able to retrieve information from that link X. Network security works by applying different kind of encryption algorithms over data before transmitting it and then it is decrypted at receiving end. From the time of wireless networks till now many approaches were proposed and implemented and then replaced by better techniques or tools. These ongoing updating of security promoted the security field to be a necessary component of the network.

A network security basically relies on the layers of protections and it includes multiple components for example as a first layer defense firewalls are used while on second level defense intrusion detection systems are used. All the components work simultaneously in order to increase the overall security of the system. To make network security more effective in performance it has to identify the threats properly and combat them by choosing the best network security tool. Some common threats to network security are [4];

- Viruses, worms, and Trojan horses
- Vandals
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Social Engineering
- Denial of service attacks
- Data interception
- Identity theft

As already mentioned that network security system consists of many components for the best result all the components have to work together to enhance security. These components includes [5]

### 2.1.1 Anti-virus software and anti-spyware software

If Anti-virus software and anti-spyware software's are updated regularly, they are able to counter most of the virus threats from the system. Antivirus and antispyware software work almost in the same way, the main difference is in the type of malicious data and pattern. The software scans the hard drive as well as the registry to detect viruses and spywares. Nowadays much antivirus software has anti-spyware software included in it or vice versa.

### 2.1.2 Firewall

Firewall blocks the unwanted access in any network. By using firewall properly in computer systems one can protect the system from harms by setting some filters that block the intrusion attempts from the hackers from Internet or from any other public or private network. Firewall can keep the log that how many times system is accessed. Firewall is a security device that can either be software or hardware implemented to any network. Firewall can perform many other functions too.

### 2.1.3 Intrusion Detection Systems (IDS)

IDS are used to monitor all the ongoing events in a network and analyze any incident which is against the network security or is a threat to network security. A more general categorization is on the basis of adopted data analysis technique. In this technique, IDS may be of the two main types. One is misuse detection and the other is anomaly detection. The misuse detection examines the whole infrastructure from attacks whereas; anomaly detection examines the protected system after some time to define what activities are normal. Any incident that considerably deviates from that kind of activities is considered an attack. It is important that IDS must detect intrusions with very high accuracy.

### 2.1.4 Intrusion Prevention System (IPS)

IPS identifies threats like zero hour attack, it has all the capabilities that an intrusion detection system (IDS) is and also it has the ability to stop the possible incident. The IPS has the ability to stop the attack by terminating the network connection, block the access of the unauthorized user, block all access to the targeted host and block the recourses. The IPS could also change the security environment by changing the configuration of their security controls to stop an attack. Few technologies can remove or replace malicious part of an attack thus IPS may also change the attack contents.

### 2.1.5 Virtual Private Network (VPNs)

VPNs provide secure access and data encryption between two peers on a network. Through VPN remote users can access the network without being hacked or intercepting data. For example it allows you to be sitting at some other place and access your company's system in the same way as if you were sitting at the company's office. It is almost impossible for the hackers to tap with data in the VPN tunnel.

### 2.1.6 Data Encryption and Network Security

Data encryption is used to ensure that original data is secured and cannot be intercepted by any unauthorized user. This is also known as cryptography. Cryptography is the most effective and a secure way to send a data via any public network or over Internet. In this technique we converted our original message with some encrypted code word by using algorithms. And on the other end the opposite peer must know the decrypted key so that to successfully decrypt the original message back

## 2.2 Swarm Intelligence

Nature always plays a vital role to solve complex human problems. In the past few years biology based techniques get the attentions of researchers. Many natural biological inspired techniques have been proposed for the network security, one of them is swarm intelligence.

Swarm intelligence is the, "The emergent collective intelligence of groups of simple agents."[6]. It is a computational intelligence approach to solve real world complex problems. It was first introduced in cellular robotics system by Beni and Wang in 1989[7]. Swarm intelligence systems buildup of a population of simple agents interactive with each other individually or with their environment. The inspiration of swarm intelligence comes from the biological or natural system. Example of SI includes ant colonies, bees, fish schooling, bird flocking and animal herding bacterial growth.

All the research, techniques, algorithms and approaches that are done up till now are after studying the behavior of swarms of insects fishes and birds. The complex problem that seems almost impossible at individual level is solved by insects, bees and birds in the form of swarms. Individually ants and bees have very limited brain and hence no intelligence but when these ants and bees interact with others to make a society then they seems to do really hard and complex tasks such as finding secure path to food, build their nests, travel in a line and synchronize their movements so that it looks like a single coherent entry with high speed etc.

This pattern becomes more significant when they doing their tasks in the absence of any centralized administrator (e.g., queen of hive). Implementation of this is seen in the NP-hard optimizations problems such as the scheduling, traveling salesman, vehicle routing etc. Researchers have done so many work in this field and create many swarm intelligence based algorithms and applications. Few important algorithms and applications are;

**Algorithms:**

- Ant colony optimization algorithm
- Artificial bee colony algorithm
- Particle swarm optimization
- Firefly algorithm
- Multi-swarm optimization
- Ant colony cluster optimization

**Applications**

- Ant-based routing
- Crowd simulation
- Swarmic art

Three main Algorithms used in network security are ACO, PSO and ACC.

### 2.2.1 Ant Colony Optimization Background

One of the main algorithms on swarm intelligence is ant colony optimization algorithm. It is based on the behaviors of ants. The inspiration of this idea is gain from the actions of ants and their ability to find the shortest secured path of food from that place to their nests. This is one of the most successful biologically inspired algorithms. Ants individually have no intelligence and without any vision. They are unable to communicate as they are deprived of the speech. However, their actions are strictly organized and well mannered. This shows that there is still some kind of communication between them.

Researches after conducting many experiments came to know that natural ants deposited a stuff known as pheromone traces, which direct others to the food recourses. Initially ants move randomly around in search of food. When they find their food they carry it to their nests and lay down pheromones traces so that others also know this path. Then the ants decided which path is the shortest and secured path to the food based on the pheromone concentration, thus they mostly choose the path that have greater concentration of pheromones.

Deneubourg et al. performs a double bridge experiment. In this experiment he separated the food material and ant's nests by a bridge, which has two branches of equal lengths[8]. He noticed that the one path is used by majority of the ants and this selection is very randomly. After this experiment Goss et al. extended this by adding two unequal lengths [9], all his experiments shows that majority of the ants choose the shortest path that is illustrated in Figure 1.

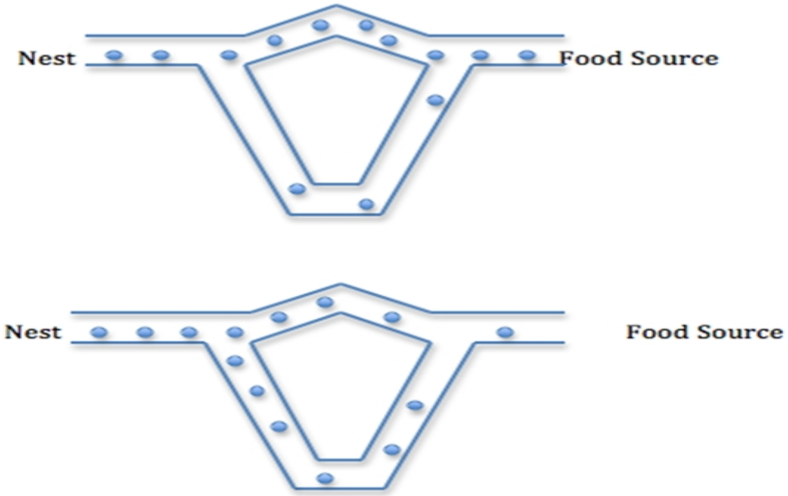

Figure 1: Extended Double Bridge Experiment

### 2.2.2 Particle swarm Intelligence Background

Particle swarm optimization (PSO) is computational method optimization technique which incorporate swarming behavior in swarms of bees, flocks of birds, schools of fish or also somehow from the human social behavior. PSO seeks inspiration [10] in the coordinated movement dynamics of birds and fishes etc. PSO proves that the kinesiology of the whole flock of birds is the result of any individual actions of a bird that follows 3 simple n basic rules.

i. Collision avoidance; which tell them to adjust their position in according to their mates.
ii. Velocity matching; which tell everyone to always synchronize their speed with the speed of their mates.
iii. Flock centering; which tell everyone to stay closer to their mates

In past few years researchers applied PSO successfully in many fields, and it also observed that PSO can give better and faster results compared to other techniques. The main strength of PSO as an algorithm is its fast and cheaper convergence, which is supposed to b more appropriate when, comparing it with other global algorithms like Genetic algorithm (GA), simulated annealing (SA) and other optimization algorithms.

Dr. Eberhart and Dr. Kennedy developed the basic PSO model in 1995[25]. According to this model a function exists. i-e $f:R^n \rightarrow R$ which is known as fitness function and it measures the quality of current solution. Inside the hyperspace a number S is randomly placed at $x_i \in R^n$ and have a random velocity $v_i \in R^n$ This particle move randomly in the hyperspace and after every step its position is evaluated according to the fitness function and speed updated by

$$v_i(t+1) = wv_i(t) + c_1r_1(p_i - x_i) + c_2r_2(g - x_i)$$

Where in above equation w denotes the constant inertia weight, $c_1$ and $c_2$ denotes the acceleration constants, $r_1$ and $r_2$ are random numbers, $p_i$ is the personal best position of particle *i*, *g* is the global best position among all particles in the swarm, and $x_i$ is the current position of particle *i*. Furthermore, the equation for the new position is:

$$x_i(t+1) = x_i + v_i(t+1)$$

The basic features of PSO model are (a) Speed and the next position of each particle is calculated according to their position of that individual with respect to the others and (b) the best solution is communicated to every other individual in the swarm. It is therefore clear that this algorithm is quite easy to implement and also researchers seeks inspiration because of the similarities between PSO and other generic algorithms. Last but not the least, PSO keep a kind of memory, which is necessary to the convergence to an optimal result.

### 2.2.3 Ant Colony Clustering

In optimization research area the ant colony clustering technique which is the extension of ant colony optimization algorithm. Many social insects such as ants and bees behaves in an amazing manner in the matter of organizing their nests arranging foods and cleaning of garbage. Research has proved that such insects have very high swarm intelligence. However, they are strict to some families of similar objects. Moreover it is observed that the highly intelligent is ants because of some their work and behavior.

One such example is they work in a group and if some external enemy attacks their nests they have the ability to reconstruct it in no time. And it has been observed that they worked voluntarily without being ordered by some administrator. On this observation many mathematical models are proposed and construct to create the cataloging and clustering behavior of the real ants. Deneubourg et al. was the first to construct a basic mathematical model on the basis of this behavior and this model is then used in robotics[11].

# 3. SWARM INTELLIGENCE IN NETWORK SECURITY

Sometimes to solve big network security problems we have to think something on a small scale, for example of an ant. One of the researches at Pacific Northwest National Laboratory is to resolve the computer-generated security problems. , Dr. Glenn Fink, one of the senior research scientists at PNNL believes that Nature always shows us paths that how can we protect networks specially computers with the help of collective intelligence. Dr. Glen together with Dr. Errin Fulp (Associate Professor of Computer Science at Wake Forest University,) works on the security software. Both the researchers studied the behavior of ant and are able to develop multiple security scanning softwares that is capable of scanning different threats.

Dr. Fulp explains the reason why they chose to copy ant’s behavior in the article “Ants vs. worms” by Eric Frazier at wake Forest University.

> *“In nature, we know that ants defend against threats very successfully. They can ramp up their defense rapidly, and then resume routine behavior quickly after an intruder has been stopped. We are trying to achieve that same framework in a computer system.”[12]*

To understand their behavior researchers watch National geographic documentaries about the ants and their colonies. They name their technology as swarm intelligence because according to definition the SI system, It is a system made from the population of birds, ants and agents interacting on simple rules with one another and also with their mates.

The researchers propose a digital swarm intelligence system. This SI system’s body consists of three main parts.[13]

**1) Digital Ant**

These are the software defined ants and have the ability to crawl in the computer code and see for the malicious data or indication of the malware. Researchers mentioned that almost 3000 different types of digital ants have to be engaged.

**2) Sentinel**

Sentinel is the autonomic administrator or manager for digital ants on a single computer. The purpose of the sentinel is to collect information from the digital ants and check the status of the local host. On the basis of this information it decides whether to take action or not. Furthermore, sentinel also reports to sergeant.

**3) Sergeant**

Like sentinel, sergeant is also an autonomic controller. But as sentinel is for digital ants, sergeant is for multiple sentinels. Number of sergeants in any network is direct with the network size, size of the network determine the numbers of sergeant for that network. It is the interface for human administrator or manager.

## 3.1 Working of Digital ANT

Working procedure of digital ant is slightly different from that of typical antivirus scanners. Different digital ants crawl in the system randomly in search of any malware. They are simply checking network statistics or programs info, process info table hence different ant population check for different areas in the same computer. When any of these agents (ANT) found something abnormal they leave their pheromone trail immediately. This attracts other ants towards that section. As the different ants are checking at different areas they start crawling towards that abnormal area. The sentinel monitors this movement and then takes action as it is trained to understand the “normal” behavior. And then sergeant approaches to sentinel and check for the changes and threats.

If the working digital ant is helpful in finding malware threats and information then more ants might be created by simple duplication. While on the other hand if it is useless it dies automatically. The population is maintained in either case. The informative digital ant is live as long as it is supplied by the reward in the form of energy. If it is unsuccessful the energy level decreases and the ant terminates. The ideas of collective intelligence of anti-virus developers is almost similar to that of swarm intelligence, the difference resides in the number of working agents.

## 3.2 Intrusion Detection Systems

Security in networks is of various types. It may be of first level defense systems such as antivirus and Trojans or might be second level defense systems that are intrusion detection intrusion prevention systems. In swarm intelligence there are number of approaches researchers found based on ant colony optimization, particle swarm optimization and ant colony clustering intrusion detection and prevention systems. Some of the work of different researchers in this area is briefly described below.

### 3.2.1 IDS approaches based on Ant Colony Optimization

As describe earlier that IDS are used to identify the worms in the networks. Fenet and Hassas are the first to propose the intrusion detection systems based on the ant colony optimization that can detect the source of attack in the system [14]. Their proposed system is based on the number of agents. They used mobile as well as static agents for this purpose. One of the necessary component, pheromone is a static server which is available at each host and is protected. One of the duties assigned to pheromone server is that it alerts the network whenever any attack is observed. This alert message is received as a pheromone of the ant. Another static agent is *watcher, which* is also available at each host and is monitoring all the processes on the host side as and its network links. Thus watcher is supposed to be the main part of the system for detection purpose. Now as far as the mobile agents are concerned *lymphocytes* are included in this part. They are always in motion and wandering different parts of the system in search of a pheromone.

The lymphocytes are mobile agents that typically roam randomly through the network searching for pheromone marks. If they found pheromone somewhere they attract towards that area and alarm the system to take action against that threat. Since the *lymphocytes* are the responsive component of the system thus this ant colony analogy is a responsive part of the systems so that intrusions can be detected effectively and fast. The complete system forms a fully distributed ID&R system. Another approach that identifies the attacks and responds to the attacks is IDReAM by[15]. In this approach the detection part is done by the inspiration of human immune system and the intrusion response system is same it works on the ant colony optimization approach.

Abadi and jalali were the first to introduced ANTNag algorithmic approach based on ant colony optimization technique for intrusion detection[16]. The idea behind their motivation was that the systems are susceptible. Intruders set free their attacks and all the possible attacks are represented by a graph called Network Attack Graph (NAG). NAG is a directed graph. The edges and paths nodes are the representation of complete attack scenario. Then with the information on these NAGs numbers of ants are created and incremented until all the area under attacked covered. For the accurate and effective results one has to analyze the susceptibility of the system accurately. However in realistic world NAG generation is a complex and difficult process.

ACO is implemented as a detection source for an attack or it also defines rules that which behavior is normal and which one is considered as abnormal.

One of another outstanding work in the field of security particularly in intrusion detection on the basis of ACO was by Soroush in 2006 [17]. He proposed a classification system based on ANT-Miner [18]. This system is inspired by the work of Parpinelli’s Ant-Miner rule extracting algorithm. The main difference of this classification is that it involves number of ant colonies instead of a single colony like other approaches of Ant-Miner. Ants are described in classes say class A and class B, then it is noticed that if some ants from class A, lost their pheromones trail and mixed with the searching of class B ants than this algorithm is put back and this situation is resolved by putting same kinds of ants in same colony. Such as if any ant leaves pheromone than only the member of that particular colony is attracted towards it. By experimenting on different colonies researcher find at last one rule for one colony. And at the end the best quality rules are added to the rules set.

### 3.2.2 IDS approaches based on Particle Swarm Optimization

Like ACO work has been done in the field of network security on particle swarm optimization techniques. Dozier et al. first proposed a PSO based system. The purpose of this system is to detect those threats or attacks that would skipped by the system's security and considered as a normal traffic [19, 20]. Majority of the PSO based IDS systems are hybrid in nature and are categorized in addition to the maximum-likelihood approaches. Some of the Hybrid PSO methods are described below.

#### *3.2.2.1 PSO based neural hybrid methods*

Researchers worked out number of application based on artificial neural network for intrusion detection purpose. Artificial neural network is supposed to be the major approach of soft computing for data classification. Artificial neural network combined with Particle swarm optimization is used widely in the field of computer security and intrusion detection. The one who combines the above-mentioned soft computing methods to form an effective intrusion

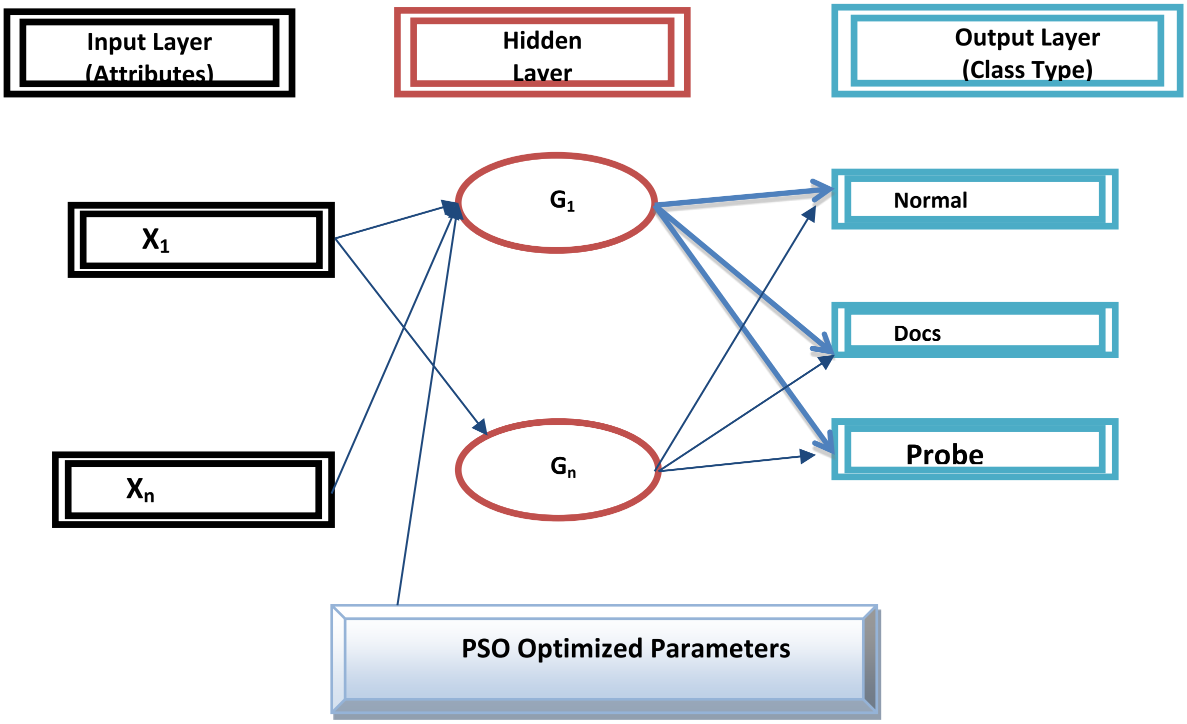

Figure 2: ANN Combined With PSO

detection [21]. They proposed an integrated intrusion detection system, which is then implemented in java. In their training duration they use PSO recursively to get the optimal results. Each element in the hybrid PSO relates to the synaptic weight (potency and amplitude) of the corresponding network. The best result synaptic weight is then sent to artificial neural network part, which then performs the classification with better effectiveness. Their system is consisting of two main parts. (a) Artificial neural network classifier, it has to complete the classification process, (b) PSO algorithm, which is running on above to train the synaptic weight and improve other important parameters, which can be easily depicted from Figure 2.

#### *3.2.2.2 Hybrid PSO and K-Means Algorithm Methods*

Xiao [22] integrate the K-Means algorithm [23] with the particle swarm optimization technique to build an effective intrusion detection system. Yongzhong also presents same kind of K-Means hybrid system with the combination of PSO [24]. This algorithm tells that position of the each element is a set of D dimensional centroids that is generated by the K-Means algorithm. Position of corresponding element is then represented by an array.

$$\begin{pmatrix} Z_{11} & \rightleftharpoons & Z_{1D} \\ \vdots & \ddots & \vdots \\ Z_{k1} & \cdots & Z_{kD} \end{pmatrix}$$

In this expression D denotes the dimensions of the centroids and k denotes the clusters. As an initial step all the data points are assigned to k number of clusters in a random way. After this assigning, centroid is calculated and each particle’s position is analyzed.

As mentioned above in the PSO section that PSO works on the basis of position and velocity thus for each element in the array , the fitness function calculates the corresponding position and velocity of the element and also update the $P_{best}$ and $G_{best}$ values of the particle. And in the end this algorithm works to optimize the new production of particles. The advantage of his algorithm is that it converges to local optimum with very low probability and it has very high convergence speed as compared to other algorithms.

## 4. CONCLUSION

Security is one the most important concern of any network whether you talk of the local Area Networks (LANs), Wide Area Networks (WANs), Metropolitan Area Networks (MANs) ,Wireless Sensor Networks (WSNs) [2]or mobile & ad-hoc Networks (MANET)[1]. Thus researchers are attacked towards this field in past few years. In this survey we briefly explain few methods, which are proposed by different scientists and researchers, of swarm intelligence optimization in network security. As the network technologies invented, security concerns are also increased. Swarm intelligence is comparatively a new technique in network security.

Swarm intelligence techniques make themselves a solid alternative for any current security techniques especially when you are talking of intrusion detection systems. Ant colony optimization (ACO) an easy to implement and fast optimization algorithm helps in the detection process of the malware. Many of the existing systems are reply on this technique in combination of some other rule based techniques. While, particle swarm optimization (PSO) and Ant colony Clustering techniques are successful techniques which provide optimal detection rate (DR). ACC is excellent in all the classes except one that is (U2R). However the main purpose of this survey is finding out the applications of swarm intelligence in network security though a very important field that is neglected up till now is the creation of distributed intrusion detection systems because security threats remain major attraction for the researchers as long as there are ways to intimidate the data in network.

## REFERENCES

[1]. Hao, Y., et al., Security in mobile ad hoc networks: challenges and solutions. Wireless Communications, IEEE, 2004. 11(1): p. 38-47.

[2]. Pathan, A.S.K., L. Hyung-Woo, and H. Choong Seon. Security in wireless sensor networks: issues and challenges. in Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference. 2006.

[3]. Williamson, M.M., Biologically inspired approaches to computer security. Information Infrastructure Laboratory, HP Laboratories Bristol, 2002.

[4]. Systems, C. What is network security. 2013 [cited 2013 March]; Available from: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html.

[5]. University, B. Network Security. 2010 [cited 2013 march]; Available from: http://www.cc.boun.edu.tr/network_security.html.

[6]. Martino, G., F. Cardillo, and A. Starita, A new swarm intelligence coordination model inspired by collective prey retrieval and its application to image alignment. Parallel Problem Solving from Nature-PPSN IX, 2006: p. 691-700.

[7]. Beni G, W.J., Swarm intelligence in cellular robotics systems, 1989: NATO Advanced Workshop on Robots and Biological System

[8]. Deneubourg, J.L., et al., The self-organizing exploratory pattern of the argentine ant. Journal of insect behavior, 1990. **3**(2): p. 159-168.

[9]. Goss, S., et al., Self-organized shortcuts in the Argentine ant. Naturwissenschaften, 1989. **76**(12): p. 579-581.

[10]. Reynolds, C.W. Flocks, herds and schools: A distributed behavioral model. in ACM SIGGRAPH Computer Graphics. 1987. ACM.

[11]. Kennedy, J. and R. Eberhart. Particle swarm optimization. in Neural Networks, 1995. Proceedings., IEEE International Conference on. 1995. IEEE.

[12]. Frazier, E. Ants vs Worms. 2009 [cited 2013 march]; Available from: http://www.wfu.edu/wowf/2009/20090921.ants.html.

[13]. Kassner, M. Swarm Intelligence: Are digital ants the answer to malware. 2009 [cited 2013 March]; Available from: http://www.techrepublic.com/blog/security/swarm-intelligence-are-digital-ants-the-answer-to-malware/2757.

[14]. Fenet, S. and S. Hassas, A distributed Intrusion Detection and Response System based on mobile autonomous agents using social insects communication paradigm. Electronic Notes in Theoretical Computer Science, 2002. **63**: p. 41-58.

[15]. Foukia, N. IDReAM: intrusion detection and response executed with agent mobility architecture and implementation. in Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems. 2005. ACM.

[16]. Abadi, M. and S. Jalili, An ant colony optimization algorithm for network vulnerability analysis. Iran. J. Electr. Electron. Eng, 2006. **2**(3): p. 106-120.

[17]. Soroush, E., M.S. Abadeh, and J. Habibi. A Boosting Ant-Colony Optimization Algorithm for Computer Intrusion Detection. in Proceedings of the 2006 International Symposium on Frontiers in Networking with Applications (FINA 2006). 2006.

[18]. He, J. and D. Long. An improved ant-based classifier for intrusion detection. in Natural Computation, 2007. ICNC 2007. Third International Conference on. 2007. IEEE.

[19]. Dozier, G., et al., Vulnerability analysis of immunity-based intrusion detection systems using genetic and evolutionary hackers. Applied Soft Computing, 2007. **7**(2): p. 547-553.

[20]. Dozier, G., et al. Vulnerability analysis of AIS-based intrusion detection systems via genetic and particle swarm red teams. in Evolutionary Computation, 2004. CEC2004. Congress on. 2004. IEEE.

[21]. Michailidis, E., S.K. Katsikas, and E. Georgopoulos. Intrusion detection using evolutionary neural networks. in Informatics, 2008. PCI'08. Panhellenic Conference on. 2008. IEEE.

[22]. Xiao, L., Z. Shao, and G. Liu. K-means algorithm based on particle swarm optimization algorithm for anomaly intrusion detection. in Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on. 2006. IEEE.

[23]. MacQueen, J. Some methods for classification and analysis of multivariate observations. in Proceedings of the fifth Berkeley symposium on mathematical statistics and probability. 1967. California, USA.

[24]. Liu, L. and Y. Liu. MQPSO based on wavelet neural network for network anomaly detection. in Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on. 2009. IEEE.