ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Particle Swarm Optimization Based Network Security Situational Awareness

[1]R.Mohanraj and [2]S.Anbu

[1]*Research Scholar, Department of Computer Science and Engineering, St.Peter's University, Avadi, Chennai, Tamilnadu, India.*
[2]*Professor, Department of Computer Science and Engineering, St.Peter's College of Engineering and Technology, Avadi, Chennai, Tamilnadu, India.*

ARTICLE INFO

Article history:
Received 23 June 2015
Accepted 25 August 2015
Available online 2 September 2015

Keywords:
Network Security Situation Awareness, Cyber Attacks, Intrusion Detection and Prevention.

ABSTRACT

The usage of network applications is increasing day by day efficiently and effectively. At the same time, various kinds of attacks are also increased. In this paper, it is aimed to provide a network security situation using PSO-Particle Swarm Optimization. PSO enables self –learning and self-adapting about the network system and increases the immunity and viability. At the time under an attack, it can be obtained that the present and the future situations around the way and it helps to take right decision and guarantee the usability of the network system. The simulation result shows the performance evaluation of PSO

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: R.Mohanraj and S.Anbu., Particle Swarm Optimization Based Network Security Situational Awareness. ***Aust. J. Basic & Appl. Sci.,*** *9(27): 56-60, 2015*

INTRODUCTION

As the usage of networks increases the problems faced by the network customers also grows bigger day-by-day. To ensure safer operation of the networks there are various technologies and algorithms for intrusion detection, virus detection and firewall are used. These technologies work in an independent way as a defensive shield for the data without any idea about the data they are protecting. This limitation of these techniques causes a phase difference in their functioning along with the data flow, which causes delay in time for the operator to understand the bug and raise the alarm. The network attacks has been almost exposed even to many amateur attackers, since the communication between people has increased vastly over the time and thus network attacks are increasing rapidly over the time.

When the network attacks first evolved the attackers used executable files with similar names, which are easily identified and stopped. As the networks got bigger and used in several applications, the network attacks have also increased and attackers have found several new ways of attacking a network. Most of the attackers use random names and different patterns for execution and hunt down the signature based intrusion detection system. Since the network security awareness is an emerging field in networks the researches are yet to reach the most researched technology marks but has attracted many expert analyst's attentions though. The researches related to network security awareness is proceeded in two ways, one concentrated on the improvement of the intrusion detection systems used and the other research concentrates on introducing the context awareness in the network security systems.

Background Study:

In order to prevent the network from attacks and improve the security of the network there are several security tools are proposed in previous work which can be used in large scale networks. These systems are designed such that they produce a lot of security events. To overcome this problem a new concept of situation awareness is introduced. This concept of situation awareness was first proposed by Bass in (Bass, T., 1999; Bass, T., 2000). He included situation awareness into the network based on multi-sensor data fusion. Endsley's (Endsley, M., 2005; Lai Jibao, *et al*., 2006) situation awareness system provides the administrator's with options to identify, track and measure. Liu *et al*. (2010) has also proposed a model for network security awareness based on information fusion. The intrusion detection systems are said to have a high number of fake alarms.

Yu *et al*. (2005) proposed a system in order to improve the performance of the intrusion detection system and enhance the situation awareness of the system the current trend of the network is studied along with the collection of fused data and their analysis. The exact settings of how to set the reliability and power of sensors is discussed in (Wang Huiqiang, Lai Jibao, and Ying Liang,

Corresponding Author: R.Mohanraj, Research Scholar, Department of Computer Science and Engineering, St.Peter's University, Avadi, Chennai, Tamilnadu, India.
E-mail: mohanresearch254@gmail.com

2007) by Wang *et al*. They also suggested the neural network for the heterogeneous multi sensor data fusion and analysis of the severity in the security situation. The positioning and analysis of sensors also play an important role in determining the current trend of the network, since their outputs determine their connectivity with the network. The analysis of warning information is also an important to reduce fake alerts. In (Dan Zerkle, et al. 2000) a latent correlation between warning information is derived by Stefanos *et al*. This process uses automatic knowledge discovery to find the correlation between warning messages. The drawback of using automatic knowledge discovery is that it may also find some utterly useless messages at times.

Bass in (Bass, T. and R. Robichaux, 2001) says that security risk factor depends on the assets of the system, threat degree and severity of attack. In (Zhang Yong, *et al*., 2007) proposed a system which considers all the environmental parameters in the situation awareness system. Chen *et al*., (2006) proposed a new method for evaluating risk factor. In (Bode Moyinoluwa A., *et al*., 2014) structures of service, network and host are considered in quantitative manipulation of the network security situation. Various methods of security situation awareness manipulation are discussed. Most of the previous works discussed a very formal model of situation awareness manipulation, but in a new integrated system is proposed by Fang Lan *et al*.

Existing System:

Bode Moyinoluwa *et al*., (2014) utilized the Bayesian Model for detecting and analyzing the security situation in a network and compared the results with the Genetic Algorithm based NSSA analysis. The author utilized the Bayes model with an Association rule mining based pattern to improve the efficiency of the attribute evaluation. The Bayesian model takes more time because of its linear searching method and it compares only a restricted pattern on the attributes. So that, the security analysis is not satisfying the customer in terms of big networks. Also, the author used KDD cup data for simulation. To improve the accuracy in verifying the network parameters, PSO based network evaluation is proposed in this paper.

Problem Statement:

From the literature survey, it is clear that various researchers proposed various techniques or algorithms for NSS. Most of the algorithms and techniques are evaluating the network parameter and checks the security. But it is necessary to design and develop an automatic self learning system for analyzing NSSA. In this paper, we provide a self service system for study about the situation awareness and use the network system. The contribution of the paper is to design and develop a PSO and deploy it in a network, which monitors and analyze the network quality.

Proposed Approach:

In this paper, the security situation is studied and intimated to the network server or to the network connection requester to take a decision using the PSO algorithm. PSO algorithm is a revolutionary programming approach, derived from the social psychological theory to solve non-linear and differential problems with multi-objectives. Since, PSO is used for searching problems, it is initialized with a population of random solutions. Each solution is called as particles and are associated with velocity. Particles fly towards better solutions in the search space, where it knows how much it is far away from the solution. PSO algorithm is simple in concept, easy to implement and it is computationally efficient.

General Schema of the proposed PSO:

1. *Initialize particles*
2. *Evaluate the fitness values of the swarm*
3. *Do*
4. *Find the personal bests*
5. *Find the global best*
6. *Update velocity of the particles*
7. *Update positions of the particles*
8. *Evaluate their fitness values*
9. *Apply local search algorithm (optionally)*
10. *Until Termination criteria are met*

PSO can do searches in a flock of agents optimizes the defined objective function. Every agent in the space knows its best value[pBest] and the best value in the flock[gBest] among the pBests.

$$V_{ij}^{t+1} = C\left[wv_{ij}^{t} + C_1 rand_1 \times \left(p_{best_i} - X_i^t\right) + C_2 rand_2 \times \left(g_{best_i} - X_i^t\right)\right]$$

$$X_i^{t+1} = X_i^t + V_{ij}^{t+1}$$

$$P_{t+1}^{k} = P_t^k + V_t$$

where, V is the velocity and P is the position, t is the time, C1 and C2 are constants as 2.

Stepwise Procedures of Proposed PSO Heuristic approach:

Step-1: Initialize a population of particles with random positions and velocities on *d* dimensions in the search space.

Step 2: Update the velocity of each particle, according to Equation (9).

Step 3: Update the position of each particle, according to Equation (10).

Step 4: Map the position of each particle into solution space and evaluate its fitness value according to the desired optimization fitness function. At the same time, update *pbest* and *gbest* position if necessary.

$\sum_{i=1}^{m}\sum_{j=1}^{n}\left(S_{ij} + n_{ij}p_{ij}\right)$// for make span

$\sum_{i=m,j=1}^{j=m}\left(S_{ij} + n_{ij}p_{ij}\right)$// for total flow time

Step 5: Go to step 2 until a criterion is matched, usually a sufficiently good fitness or a maximum number of iterations.

The population size has almost no significant effect on the performance of the PSO. However, there is a slight improvement of the optimal value with increasing swarm size, usually the number of particles is in the range 20–60. Therefore, in this work the swarm size is set to 40 particles for all experiments. In PSO the balance between the global and local exploration abilities is mainly controlled by the weighting function. The role of the initial Weight *(*Wi*)* and final Weight *(*Wf *)*is considered critical for the performance of PSO. The weighting function is used to control the impact of the previous velocity of particle on its current velocity. In addition, the weighting function regulates the tradeoff between exploration and exploitation abilities of the swarm. Where a large inertia weight facilitates global exploration and a small one tends to facilitate local exploration. The entire functionality of the PSO algorithm is given in Fig.1 blow.

Flowchart of PSO:

In this paper the PSO is acting as a distributed agent deployed in the central. All the information about the security situation of the subordinate sub-networks and the individual computers are evaluated by the PSO. Then network risks are analyzed like type, quantity, strength and harmful of the attacks. PSO itself is an SSA system, which can process in iterations and mainly monitors the network host's behavior. Because the behavior like control, subnetwork, speaking, answering and request-response time sharing with other host on the network. The main factors learned PSO are IP, packet size, time, memory and defense capability of the each node.

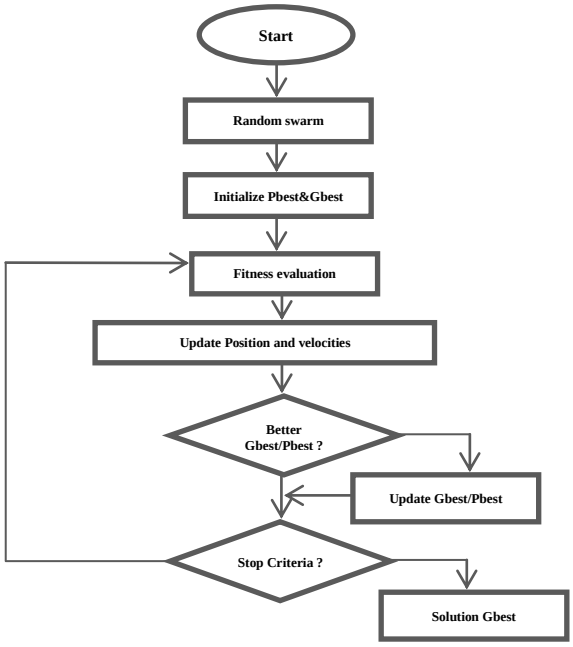

Fig. 1: Flowchart for PSO Solving NSSA

The s*et al*l attributes $\boldsymbol{A} = \{\boldsymbol{A_1}, \boldsymbol{A_2}, \ldots, \boldsymbol{A_k}\}$[Network Parameters]. The objective function given in the PSO algorithm is

$$\left\{\prod_{i=1}^{k} \boldsymbol{A_i} \geq \boldsymbol{Th_{Ai}} \ \boldsymbol{then} \quad \boldsymbol{Access\ permitted} \right\}$$
$$\boldsymbol{else\ Access\ Denied}$$

All the attributes of the network are assigned in the objective function to verify whether it meets the constraint or not. If the attributes meet the constraint then the network can be selected and it can be connected. Else the network is rejected for the connection. All the attributes are recorded during the network connection and are evaluated by PSO and find the best network for connecting dynamically. The evaluation of the network is carried out in term of attributes and the threshold value of the attributes assigned. The threshold value is assigned manually or automatically in the PSO implementation.

RESULT AND DISCUSSION

The Multi-stage precaution information methodology is simulated in a college Laboratory having more than 250 computer systems. Lab is installed with Windows-7 operating system; Airtel based WiFi internet connection and more hardware

and software resources. It is noticed that all kind of secured transactions is happening in the internet like bank transaction in the office, student data transaction between the college and the university and so on. All the transactions make in the college is more important and need more security. To do simulation about the proposed approach, a system monitoring software is installed and analyzed about the systems and the system behavior. According to our evaluation strategy, and the constraints applied some of the systems are identified as bad systems due their request applied in the internet as well as in the intranet. The entire details of the simulation data and the identification of bad system are given in Table-1.

Table 1: Classification of Network and Attacks

Number of Network Connection	Number of Attack	Category	Types of Attacks	Correctly Identified	Incorrectly Identified
20	4	Back	DOS	4	0
40	7	IPSweep	Probe	6	1
20	2	Perl	U2r	2	0
10	3	ftp_write	R2l	1	2

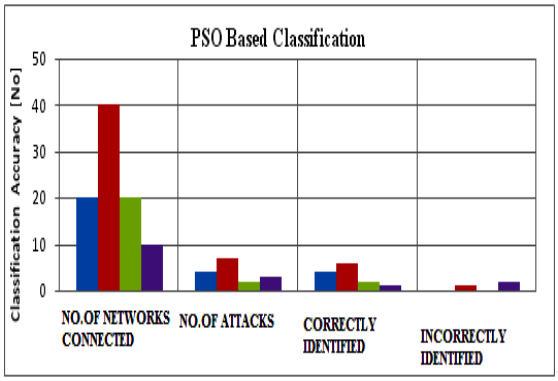

Fig. 2: PSO Based Classification On NSSA

A portion of the data taken from (Bode Moyinoluwa A., *et al*., 2014), input to PSO algorithm. The PSO algorithm investigate and evaluate the network parameters and classify the networks is Secured or unsecured. According to the classification PSO proves that it can evaluate the network security situation awareness in a better manner than the other existing approaches.

Conclusion:

In this paper the main objective of the paper is to analyze the given network is having security by comparing the network security situation analyzation factors using Particle Swarm Optimization approach. In this paper the attribute values are compared with the personal best and global best values and reach the solution very fast and effectively. It is necessary to check the network situation before going to connect with any kind of e-business nowadays. The existing approaches directly mapping the input values with the trained values. But, in this paper, the PSO search and find out the best values for connection. Since this paper can provide an efficient approach for analyzing the network security situation awareness.

REFERENCES

Bass, T., 1999. "Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems ", IRIS National Symposium on Sensor and Data Fusion, pp: 24-27.

Bass, T., 2000. "Intrusion Detection Systems and Multisensor Data Fusion", Communications of the ACM, 43.

Endsley, M., 2005. "Toward a theory of situation awareness in dynamic Stage S Possible DDoS Attacks ystems ", Human Factors, 37: 32-64.

Lai Jibao, Wang Huiqiang, and Zhu Liang, 2006. "Study of Network Security Situation Awareness Model Based on Simple Additive Weight and Grey Theory.

Fang Lan, Wang Chunlei, MaGuoqing, 2010."A Framework for Network Security Situation Awareness Based on Knowledge Discovery", Computer Engineering and Technology, 2nd International Conference, V1-226 - V1-231.

Yu Dong and Frincke, D., 2005. "Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory ",ACM Southeast Conference.

Wang Huiqiang, Lai Jibao, and Ying Liang, 2007. "Network Security Situation Awareness Based on Heterogeneous Multi-Sensor Data Fusion and Neural Network", Second International Multi symposium on Computer and Computational Sciences.

Stefanos Manganaris, Marvin Christensen, Dan Zerkle, et al. 2000.“ A data mining analysis of RTID alarms”, Computer Networks, 34: 571-577.

Bass, T. and R. Robichaux, 2001. "Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations, " Proceedings of IEEE Military Communications Conference, 1: 64-70.

Zhang Yong, Tan Xiaobin and Xi Hongsheng, 2007."A Novel Approach to Network Security Situation Awareness Based on Multi-perspective Analysis, "IEEE 2007 International Conference on Computational Intelligence and Security.

Chen, X.Z., Q.H. Zheng and X.H. Guan et al., 2006. "Quantitative hierarchical threat evaluation model for network security", Journal of Software, 17(4): 885-897.

Bode Moyinoluwa A., K. Alese Boniface, F. Thompson Aderonke and IyareOtasowie, 2014.” A Bayesian Network Model for Risk Management in Cyber Situation”, WCECS 2014, 22-24.