IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 11, November 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

An Improved PSO Algorithm for DDOS Attack Detection in Wireless Networks

R.Basheer Mohamed [1], Dr.S.Arumugam [2]

[1] Associate Professor, Department of IT, Indra Ganesan College of Engineering, Trichy, Email:profbasheer19021977@gmail.com

[2] Professor, Department of CSE, Nandha Engineering College, Erode, Email: arumugamdote@yahoo.co.in

Abstract: With rapid increase in communication technologies and protocols for online communication, as equal and even more dangerous threat in from of hacks and attacks have been prevalent which pose serious consequences to transaction based firms and concerns. One such attack identified in the literature is the distributed denial of service attack (DDoS). Given a large pool of resources to process with, denial of service attacks prevent the user from exploiting the full capacity of available resources resulting in congestion or traffic in the network. Numerous research contributions have been observed in the literature in which particle swarm optimization technique to effectively deal with detection of incoming DDoS attacks has been investigated and presented in this paper.

Keywords: Network attacks, denial of service, particle swarm optimization

I. INTRODUCTION

The role of internet in day to day affairs in both commercial and industrial sectors has grown in leaps and bounds. At the same time the intensity of attacks have grown at the double amount comparatively to aid in illegal access, tampering of data over the network, manual congestion of traffic etc., One of the most disturbing type of attacks [5] [12] is the distributed denial of service attacks which pose a severe nuisance to users as they are basically exposed to a very slow or no internet access at all. Subsequently these faults cause severe financial crisis due to loss of millions of revenue [9] due to lack of adequate internet services. They also cause serious threats to the safety and security of confidential information in a nation's interest by attacking the governmental websites [2]. Hence, it is essential to eliminate or at least reduce the damage caused by denial of service attacks. A typical DDoS scheme of attack is depicted in figure 1.

The figure 1 illustrates the attack scheme of a DDoS over the internet which directly targets the end user server. The malicious packets are mixed with the true data by the hackers and fed into the internet which poses serious unavailability problems to the end users [7]. The DoS attack detection system should be self adaptive in nature capable of detecting a wide range of dynamically varying infected packets approaching the target server. In spite of the requirement that the proposed system should be self adaptive in nature, it should also be available at a reduced computation cost and complexity [12][14-16]. A serious drawback observed in the literature is that the existing algorithms have not been effectively able to deal with new variants of DDoS attacks. The proposed system architecture [11] should aid in extracting the characteristics of the networks in deriving a perfect geometrical correlation between the traffic features. Efficiency of the proposed architecture would be improved by introducing independency of the system component on prior knowledge about the nature of attack.

A DDoS attack occurs in a phased manner with the initial objective as to set up an agent node. These nodes replicate as multiple agents and continuously scan the virtual machines in the network for any loophole in the security mechanism [5] of the target machine. The attack codes are injected into the holes of the target machines and the infected machines could now recruit new multiple agents. A distributed attack is a slight variant where the infection methodology is distributed over the network on the pretext of a very useful and essential application.

Figure 2 gives an illustration of the attack mechanism through with the infected packets are delivered over the network to the desired target. A brief survey of literature indicates several contributions in detection of DDoS attacks ranging from evolutionary computing algorithms like optimization techniques involving natural phenomena [7][11], artificial neural network models [2] [4] [17] which are aimed at training the model to the given problem objective and cluster based techniques [8][13]. The rest of the paper is organized into a brief illustration of PSO in section II followed by the proposed algorithm in section III. Section IV gives the findings of the experimentation with the conclusion drawn in section V.

II. PARTICLE SWARM OPTIMIZATION (PSO)

The particle swarm optimization algorithm is a well known stochastic and optimization based algorithm proposed by Kennedy et al. PSO is known for its fast computation speed and has found extensive utility in training, estimation, detection,

classification and recognition application over a wide range of disciplines. Particle swarm optimization is based on the concept of particles which are set in motion through packets of information received from the surrounding environment of the node under study. The degree of successful solution obtained by each particle is specified through its merit function. An optimized solution towards the desired problem objective is achieved of migration of these particles towards particles with higher degree of merits thus converging upon an optimized solution.

Given any objective function of optimization by PSO, a random space is created with an arbitrary number of particles with initial merit functions. It is an iterative and stochastic method where each particle moves towards a higher merit particle in the solution space. During the migration or movement of these particles, essential parameters like position, speed, and velocity of the particle are directly influenced with help in modeling of PSO solution. The position of the particle is closely correlated to the most optimal orientation of the particle during migration.

The position and the current velocity of the particle play a key role in modeling a iterative model for optimality in the objective function. The swarm of particles is observed to be continually oscillating with no settling point once they are set off in motion. The oscillations occur surrounding the minima function of the given objective function. The position of the particle at any point of time *t* is defined by the vector set given by

$$p_n = [p_1, p_2, p_3, p_4 \dots \dots . . p_{nt}] \quad (1)$$

The population consisting of the swarm of *i* particles is given by

$$P = \{P_1, P_2, P_3, P_4 \dots \dots . P_N\} \quad (2)$$

As mentioned above, the trajectories of the particles in motion governed by the model equation given as

$$p_i\,(n+1) = \; p_i\,(n) + \; s_i(n+1) \quad (3)$$

In (3) *n* and *n+1* denotes the iteration instants and s_i denotes the swarm function or the particle collecting efficiency. The above equation governs the movement of the particles across the search space towards optimal solution. Three critical parameters are defined with respect to movement of the particles namely inertia, cognitive component and social component. The first parameter is responsible for keeping the particle moving at a gradual variation in orientation rather than exhibiting sudden change in its position. It is based on feedback from previous direction data during movement. The second parameter keeps track of the movement of particles back to their previous best solutions in the search space while

the last parameter defines the tendency of the particle to move towards the local neighbourhood of the particle. Based on the above facts, the iteration process is governed by the equation

$$v_i(n+1) = v_i(n) + a_1\left(b_p - p_i(n)\right)M_1 + a_2\left(b_g - p_i(n)\right)M_2 \qquad (4)$$

where b_p is the so called "personal best" of the particle constituted by the set of coordinates for the best solution obtained so far by that specific individual, while b_g is the "global best" which defines the overall best solution obtained by the swarm. The acceleration constants a_1 and a_2, which are real-valued and usually in the range $0 \leq a_1, a_2 \leq 4$ are called "cognitive coefficient" and "social coefficient". On the other hand, M_1 and M_2 are two diagonal matrices of random numbers generated from a uniform distribution in [0, 1]. Based on the above set of governing equations and iteration procedures, the algorithm for PSO convergence could be summarized as

Step 1: Define the problem space for optimizing the given objective function

Step 2: Initialize the parameters for modelling the PSO for iteration

Step 3: Initialize the position of the particle

Step 4: Assign the position to the initial position of particle.

Step 5: Generate a randomly defined population P

Step 6: Run the PSO for predefined number of iterations.

Step 7: Compute the merit function associated with each particle in P.

Step 8: Determine b_p and b_g for each particle

Step 9: Evaluate the fitness of each particle.

Step 10: Update the merit function based on iterative computation of position and velocity.

Step 11: Check for stop solution based on convergence for final solution

Step 12: If stop solution not met, then go to set 6.

The figure.3 clearly depicts the migration process of the particles towards the optimal solution after initialization of the particles with their associated merit functions. At the n^{th} iteration, the swarm of particles converges to the optimal solution thus meeting the problem objective. The optimality of solution increases with the density of the swarm of particles surrounding the optimal solution.

III. PROPOSED ALGORITHM

This section of the paper elaborates the proposed algorithm for improved PSO convergence for detection of DDoS attacks. DDoS attacks pose to be a major challenge in depleting the resources from the system as well as the online resource pool. Hence an efficient defence mechanism is required to address and countermeasure the DDoS attacks and restore the computational efficiency of the system under attack in the quickest time possible. The proposed model for implementation of PSO based DDoS defence system is shown in figure 4.

The proposed architecture is based on TCP protocol as it is being currently employed in almost all online communication and remains to be the integral part of internet services over a long period of time. This section addresses an improved PSO algorithm for DDoS attacks which provide devastating effects on the victim machine. They result in a large number of unanswered information packets which are mainly sync signals leading to unwanted traffic on the network. The communication mechanism using a TCP mechanism is depicted in figure 4 which establishes between the source and destination for packet transfer using three signals namely *sync*, *sync-ack* and *ack*. The process starts with transmission of *syn* to the destination. On reception of this *sync* signal, the destination and source are established in connection through the TCP protocol. The connection is established through *sync-ack* signal and is partial in nature at this stage.

As depicted in the figure 5, the last process is transmission of *ack* packet to the receiver on obtaining the *syn-ack* signal from the receiver. The destination now hands over control over all its resources to the source requesting the service and the full open connection is established between the source and destination. DDoS attack in this condition occurs when the receiver or victim sends multiple *sync-ack* based on the multiple *sync* packets sent from the attacker. This occurs in the environment when the attacker spoofs the internet protocol address. This huge simultaneous non-synchronized and unnecessary exchange of information results in traffic congestion over the network resulting in system hang and crash.

In the proposed algorithm, given that values of t and c which represent the time and connection established are taken to be the important design parameters in design of DDoS attack detection and defence model. The proposed algorithm is summarized below which dynamically tunes towards the best solution which is analogous to the defence position.

The DDoS attack causes over flooding of the network causing a jam in the network speed and bandwidth. The proposed algorithm for detection is summarized below

Input: node status q_1 ->q_{n-1}

Target: alarm signal a_p on detection of DDoS

If (q_i_status = true) then

int_mac_q_i = get_ add r_{xx} ()

If (int_mac_ q_i is in intruder)

*then /*Check Intruders' List*/ (Ignore the request)*

else if (int_mac_ q_i is in true client)

check true Clients' List/ (Ignore login request)*

and (store int_mac_ q_i in intruder)

*else if (int_mac_ q_i is in client) then /*Check Client's List*/ (Ignore the request)*

end if

end if

end if

stop

end

Input: Message text from $n_1 \epsilon$ 0 to n-1node

Target: Best fit

Compute p = ab

Determine Φ (p) = Φ (a) Φ (b)

Begin

Compute q = n_1 e mod p . //e computed from Φ (p)//

$$v_i(n+1) = v_i(n) + a_1\left(b_p - p_i(n)\right)M_1 + a_2\left(b_g - p_i(n)\right)M_2$$

Return q

end

The proposed defence scheme aims to minimize number of lost connections and to prevent the system from allocating buffer space to attack connections. In the other word, the defence scheme is an optimizer that tries to minimize P_{loss} which indicates the probability of connection loss and maximize the degree of regular requests buffer occupancy. P_{loss} is connection loss probability, a basic measure for assessing the performance of the system

under DDoS attacks. Each arriving connection request packet must be dropped once there have already been m pending connections in the system. Therefore P_{loss} can be described as the ratio of the number of dropped requests to the all arrived requests. The final part is to perform an appropriate mapping between problem solution and PSO particle. For this purpose we represent the PSO particle position as *(t,c).* The flow process is depicted in figure 6.

IV. RESULTS AND DISCUSSION

The proposed system is tested on a Celeron processor 1.85 GHz with 2GB RAM running Windows XP and coded by Matlab 6.5. KDD Cup 99 has been used for the experimentation and benchmarking purpose in this testing. Each TCP connection has 60 features with a label which specifies the status of a connection as either being normal, or a specific attack type. There are 47 numeric features and 3 symbolic features falling into the following four categories:

- Basic features: 9 basic features are used to describe each individual TCP connection.
- Content features: 13 domain knowledge related features are used to indicate suspicious behaviour having no sequential patterns in the network traffic.
- Time-based traffic features: 9 features are used to summarize the connections in the past 2 s that have the same destination host or the same service as the current connection.
- Host-based traffic features: 10 features are constructed using a window of 100 connections to the same host instead of a time window.

Seven features namely *src_bytes, dst_bytes, count, srv_count, dst_host_count, dst_host_srv_count, dst_host_same_src_port_rate* have been chosen for the experimentation. The dataset contains about five million connection records as training data and about two million connection records as test data. 952 records have been chosen to limited data size.

The figure 7 illustrates the variation of attacks simulated in the proposed algorithm. The attacks have been purely DDoS attacks only targeted over a period of time varying from 200 to 7000s on the target or victim server. It could be seen that the pattern is quite unpredictable and hence the proposed algorithm should be able to self adapt towards this dynamically varying attack patter. The resource manager depicting the detection of true and false DDoS packets are depicted in figure 8

The variation of particle size against the number of iterations depicting the effect of the number of particle population on the swarm evolution is depicted in figure 9.

The results have been observed for varying particle number of 20 and 100 analysing the changes in the fitness of the global best of the swarm at each iteration. The number of iterations observed in the paper is 350, 339 and 347 for the three distinct population categories. A plot of convergence of the proposed improved PSO (IPSO) is obtained and analysed against existing PSO convergence techniques. The variation plot has been depicted in figure 10

A tabular analysis has also been carried out by listing out the measured mean and best fit values and compared against the existing PSO technique. The observations are tabulated in table 1. Three fitness merits have been utilized and it could be evident from the table that the proposed improved PSO outperforms the conventional existing techniques in obtaining the best fit for the particle in detecting the DDoS.

The efficiency of the proposed work has been evaluated in terms of detection rate (DR), true positive rate (FPR) and False Negative Rate (FNR) and tabulated as depicted in table 2. It could be seen from the above table that the proposed PSO algorithm outperforms the conventional technique in terms of the detection rate thus vindicating the efficiency of the proposed algorithm. The fitness update based on position and velocity accounts for this elimination of unwanted detection of false alarms. Figure 11 depicts the plot of computation time for the proposed IPSO algorithm over the number of iterations. The green plot indicates the proposed IPSO while the red trace indicates the variation of existing PSO.

It could be seen from the above plot that as the iteration number increases especially for large quantities of DDoS packets received at the PSO module, the computation time drastically reduces in comparison to existing optimization technique.

V. CONCLUSION

This research paper has clearly elaborated the various features of the DDoS attacks which are quite essential in designing and implementing an efficient detection and defense system. The proposed algorithm has been compared with existing PSO algorithm and the experimental results indicate marginally superior performance of the proposed position based PSO algorithm. The proposed algorithm has been modified with respect to the topology of implementation. The proposed algorithm and experimental results have been compared against the standard PSO algorithms and are found to outperform with less number of

iterations for convergence of error function. This consequently has a direct bearing on reducing the computational complexity and cost.